Sun Java System Communications Services 6 2005Q4 Delegated Administrator 指南

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

文件號碼：819–4106
2005 年 10 月

目錄

表清單

圖清單

前言

本指南說明如何配置與管理 Sun ™Sun Java System Communications Services Delegated Administrator。本指南同時也說明了 Delegated Administrator 指令，並提供語法及範例。

Delegated Administrator 由一個主控台 (圖形化使用者介面) 以及一組指令行工具組成，用於使用 Sun Java System Access Manager 佈建 Sun Java System Messaging Server 和 Sun Java System Calendar Server 使用者、群組、網域和資源。

本章涵蓋的主題有：

本書適用對象

如果您負責在站點管理、配置和部署 Delegated Administrator，請參閱本書。

閱讀本書之前

本書假設您負責管理本軟體，並對以下內容有基本瞭解：

- 網際網路和全球資訊網
- Messaging Server 協定
- Sun Java System Administration Server
- Sun Java System Directory Server 和 LDAP
- Sun Java System Console
- 在以下平台上進行系統管理和網路作業：
  - Solaris 8 (SPARC 以及 x86)
  - Solaris 9 (SPARC 以及 x86)
  - Solaris 10 (SPARC 以及 x86)
  - HP-UX 11.x
  - Windows 2000

  一般部署架構

本書架構

下表概括本書內容。

表 P–1 本書架構

章	說明
第 1 章	說明 Delegated Administrator 提供的目錄組織、管理員角色以及服務套裝軟體
第 2 章	說明安裝和配置 Sun Java System Communications Services Delegated Administrator 的必要步驟。
第 3 章	說明 Delegated Administrator 配置程式及其使用步驟。
第 4 章	說明如何自訂 Delegated Administrator，例如，變更主控台的外觀感覺。
第 5 章	說明 `commadmin` 公用程式，並提供語法及範例。
附錄 A	說明服務提供者管理員角色以及由其管理的提供者與企業組織。

表 P–1 本書架構　（續）

章	說明
附錄 B	列出了特定指令行選項的屬性值和時區值。
附錄 C	列出了可以檢查用於對 Delegated Administrator 進行除錯的記錄檔。
附錄 D	爲 Delegated Administrator、Web 容器 和 Directory Server 提供調校提示，用以提昇 Delegated Administrator 效能。
附錄 E	說明如何合併 ACI 以及如何從目錄中移除未使用的 ACI。

相關書籍

`http://docs.sun.com` SM 網站可讓您存取 Sun 線上技術文件。您可以瀏覽歸檔檔案或搜尋特定書籍標題或主旨。

Messaging Server 文件

使用以下 URL 查看所有 Messaging Server 文件：

`http://docs.sun.com/coll/1312.1`

以下列出了可用的文件：

- Sun Java™System Messaging Server Administration Guide
- Sun Java™ System Messaging Server Administration Reference
- Sun Java™ System Messaging Server MTA Developer's Reference
- Sun Java™ System Messenger Express Customization Guide

Messaging Server 產品套件包含其他產品，例如 Sun Java™ System Directory Server 和 Administration Server。這些以及其他產品的文件可以在下列 URL 中找到：

`http://docs.sun.com/db/prod/sunone`

除軟體文件之外，請參閱 Messaging Server 軟體論壇，以取得有關特定 Messaging Server 產品問題的技術說明。可經由以下 URL 造訪該論壇：

`http://swforum.sun.com/jive/forum.jsp?forum=15`

Calendar Server 文件

使用下列 URL 來查看全部的 Calendar Server 文件：

`http://docs.sun.com/coll/1313.1`

以下列出了可用的文件：

- Sun Java™ System Calendar Server Administration Guide
- Sun Java™ System Calendar Server Developer's Guide

Communications Services 文件

使用以下 URL 之一查看適用於所有 Communications Services 產品的文件：

`http://docs.sun.com/coll/1312.1`

或者

`http://docs.sun.com/coll/1313.1`

以下列出了可用的文件：

- Sun Java™ System Communications Services Release Notes
- Sun Java™ System Communications Services Delegated Administrator Guide
- Sun Java™ System Communications Services Deployment Planning Guide
- Sun Java™ System Communications Services Schema Migration Guide
- Sun Java™ System Communications Services Schema Reference
- Sun Java™ System Communications Services Event Notification Service Guide
- Sun Java™ System Communications Express Administration Guide
- Sun Java™ System Communications Express Customization Guide

協力廠商網站參照

本文件中提供了協力廠商 URL 以供參考，另亦提供其他相關的資訊。

備註 – Sun 對本文件中提到的協力廠商網站的可用性不承擔任何責任。對於此類網站或資源中的 (或透過它們所取得的) 任何內容、廣告、產品或其他材料，Sun 並不表示認可，也不承擔任何責任。對於因使用或依靠此類網站或資源中的 (或透過它們所取得的) 任何內容、產品或服務而造成的、名義上造成的或連帶產生的任何實際或名義上之損壞或損失，Sun 概不負責，也不承擔任何責任。

文件、支援和訓練

Sun 功能	URL	說明
文件	http://www.sun.com/documentation/	下載 PDF 和 HTML 文件以及訂購印刷文件
支援和訓練	http://www.sun.com/supportraining/	取得技術支援、下載修補程式以及瞭解 Sun 課程

存取 Sun 線上資源

如需產品下載、專業服務、修補程式與支援和其他開發者資訊，請至下列位址：

- 下載中心 http://wwws.sun.com/software/download/
- 專業服務 http://www.sun.com/service/sunps/sunone/index.html
- Sun 企業服務、Solaris 修補程式和支援 http://sunsolve.sun.com/
- 開發者資訊 http://developers.sun.com/prodtech/index.html

聯絡 Sun 技術支援

如果您在本文件中找不到所需之本產品相關技術問題的解答，請至：http://www.sun.com/service/contacting。

印刷排版慣例

下表描述本書在印刷排版上所做的變更。

表 P–2 印刷排版慣例

字體*	意義	範例
`AaBbCc123`	指令、檔案與目錄的名稱，以及電腦螢幕畫面輸出	請編輯您的 `.login` 檔案。 請使用 `ls -a` 列出所有檔案。 `machine_name% you have mail.`
`AaBbCc123`	您所鍵入的內容(與螢幕畫面輸出相區別)。	`machine_name%` **`su`** `Password:`
AaBbCc123	將用實際的名稱或數值取代的變數。	要刪除檔案，請鍵入 `rm` *filename*。
術語強調變數	新的字彙或術語、要強調的詞。	**快取記憶體**是儲存在本機的副本。 請**不要**儲存此檔案。
「AaBbCc123」	用於書名及章節名稱。	請閱讀「使用者指南」中的第 6 章。

* 瀏覽器中的設定可能會與這些設定不同。

指令範例中的 Shell 提示符號

下表顯示 C Shell、Bourne Shell 和 Korn Shell 的預設系統提示符號以及超級使用者提示符號。

表 P–3 Shell 提示符號

Shell	提示符號
C Shell 提示符號	`machine_name%`
C Shell 超級使用者提示符號	`machine_name#`
Bourne Shell 和 Korn Shell 提示符號	`$`
Bourne Shell 和 Korn Shell 超級使用者提示符號	`#`

符號

下列表格描述本書中採用的符號慣例。

表 P–4 符號慣例

符號	說明	範例	意義
`[ ]`	含有選用的指令選項。	`ls [-l]`	不需要 `-l` 選項。
`{ | }`	含有一組適用於所需指令選項的選擇。	`-d {y|n}`	`-d` 選項要求您使用 `y` 引數或 `n` 引數。
-	同時按下多個按鍵。	Control-A	當您按住 Ctrl 鍵時按下 A 鍵。
+	連續按下多個按鍵。	Ctrl+A+N	按住 Ctrl 鍵，放開它，然後按下後續的鍵。
>	表示選取圖形化使用者介面上的功能表項目。	[檔案] > [新增] > [範本]	從 [檔案] 功能表中，選擇 [新增]。從 [新增] 子功能表中，選擇 [範本]。

預設路徑及檔案名稱

下列表格描述本書中使用的預設路徑和檔案名稱。

表 P–5 預設路徑及檔案名稱

專有名詞	說明
msg_svr_base	代表 Messaging Server 的基底安裝目錄。*msg_svr_base* 安裝的預設值如下： Solaris ™ 系統：`/opt/SUNWmsgsr` Linux 系統：`/opt/sun/messaging`
da_base	表示 Delegated Administrator 的基底安裝目錄。 *da_base* 安裝的預設值如下： Solaris ™ 系統：`/opt/SUNWcomm` Linux 系統：`/opt/sun/comms/commcli`

Sun 歡迎您提出寶貴意見

Sun 致力於提高文件品質，因此誠心歡迎您提出意見與建議。

若要分享您的意見，請至 `http://docs.sun.com`，並按一下 [Send Comments (傳送您的意見)]。在線上表單中，請提供文件標題和文件號碼。文件號碼是一個七位或九位的數字，可以在書的標題頁面或文件的頂部找到。例如，本書的標題是「Sun Java System Communications Services 2005Q4 Delegated Administrator 指南」，文件號碼是 819-4106。在您提出意見時，可能需要在表單中輸入英文版書名和文件號碼，本書的英文版文件號碼和書名爲：819-2658 和「Sun Java System Communications Services 6 2005Q4 Delegated Administrator Guide」。

第 1 章

Delegated Administrator 簡介

Communications Services Delegated Administrator 公用程式和主控台可讓您在 Communications Services 應用程式 (如 Messaging Server 和 Calendar Server) 使用的 LDAP 目錄中佈建使用者、群組、網域和資源。

本章說明以下主題：

簡介

使用 Delegated Administrator，您可以將佈建作業分配給較低階管理員，其具有管理 LDAP 目錄中指定組織的權限。委託使用者管理功能具有以下優點：

- 將可能很費時的大型目錄佈建作業分配給多個管理員。數十個或數百個管理員可以管理可能包含數以千計或數以百萬計使用者的目錄中的組織。
- 可讓您在可做爲明確 (或唯一) 的單位管理和佈建的目錄結構中建立組織。這些組織可以包含屬於用戶商務、公司部門或其他群組的使用者。

Delegated Administrator 提供兩個用於在目錄中佈建使用者和組織的介面：

接下來的小節中概述了這兩個介面。

Delegated Administrator 公用程式

Delegated Administrator 公用程式是一組指令行工具，用於佈建 Messaging Server 和 Calendar Server 組織、使用者、群組和行事曆資源。

備註 – Delegated Administrator 公用程式提供之前發行版本的 Communications Services 產品 (Messaging Server 6 2005Q1 和 Calendar Server 6 2005Q1) 中提供的指令行功能。Delegated Administrator 公用程式不提供用於建立本書中所述的服務提供者角色和組織的指令。若要建立並管理這些新角色和組織，您必須使用 Delegated Administrator 主控台。

您可以使用 `commadmin` 指令呼叫公用程式。

如需有關 `commadmin` 公用程式提供的語法和選項的資訊，請參閱第 5 章

Delegated Administrator 主控台

Delegated Administrator 主控台是用於佈建 Messaging Server 和 Calendar Server 組織、使用者、群組和行事曆資源的圖形化使用者介面 (GUI)。

如需有關如何使用主控台的資訊，請參閱 Delegated Administrator 主控台線上說明。

Delegated Administrator 和 LDAP 目錄

Delegated Administrator 可讓您透過修改 LDAP 目錄來佈建使用者。您無需直接修改目錄。但是，瞭解增加至目錄中使用者項目和較高階節點的 Delegated Administrator 屬性可能會很有用。

如需有關支援 Delegated Administrator 的 LDAP 模式物件類別和屬性的資訊，請參閱「*Sun Java System Communications Services Schema Reference*」中的「Chapter 5:Communications Services Delegated Administrator Classes and Attributes (Schema 2)」。

佈建使用者的方案

根據業務需要，您可以建立由單個管理員管理的簡單目錄結構，也可以建立多階式目錄階層，其中的佈建和管理作業委託給較低階的管理員。

本小節概述了複雜性循序遞增的三個方案。然後說明 Delegated Administrator 提供以支援這些方案的需求的管理員角色和目錄結構。

一階式階層

在此方案中，一個公司或組織可以支援數以百計或數以千計的雇員或使用者。所有使用者都分組在單個組織中。單個管理員角色檢視和管理整個群組。此方案不存在委託管理作業。

圖 1–1 顯示了單個組織，一階式階層中的管理員角色範例。

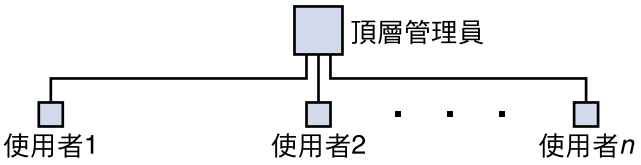

圖 1–1 一階式階層中的管理員角色

在此一階式階層中，管理員稱爲頂層管理員 (TLA)。

在圖 1–1 所示的範例中，TLA 直接管理和佈建使用者 (使用者1、使用者2、直到使用者n)。

如果您的目錄中有一個組織，則 TLA 爲您所需要的唯一管理員。

如需更多資訊，請參閱以下各小節：

- 第 25 頁的 「支援一階式階層的目錄結構」
- 第 27 頁的 「頂層管理員角色」。

兩階式階層

在此方案中，大型公司如某個網際網路服務提供者 (Internet Service Provider, ISP) 可爲企業提供服務。每個企業都有其自己唯一的網域，其中可能包含數以千計或數以萬計的使用者。

此方案支援將作業委託給較低階的管理員，而不是依賴單個頂層管理員 (TLA) 管理和佈建所有網域。

在兩階式階層中，目錄中包含多個組織。其爲每個託管網域建立一個獨立的組織。

爲每個組織都指定一個組織管理員 (OA)。OA 負責該組織中的使用者。OA 無法檢視和修改其自己的組織之外的目錄資訊。

圖 1–2 顯示了兩階式階層中管理員角色範例。

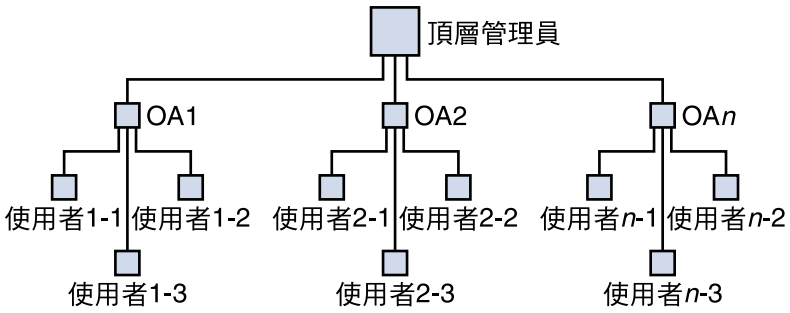

圖 1–2 兩階式階層中的管理員角色

在圖 1–2 所示的範例中，TLA 建立並管理 OA1、OA2、直到 OAn。每個 OA 管理一個組織中的使用者。

如果您的目錄中需要多個組織，則應建立 TLA 和 OA 以管理這些組織及其使用者。

如需更多資訊，請參閱以下各小節：

- 第 27 頁的 「支援兩階式階層的目錄結構」
- 第 27 頁的 「頂層管理員角色」
- 第 28 頁的 「組織管理員角色」 。

三階式階層

在此方案中，一個公司 (如 ISP) 可爲數以百計或數以千計的小型企業提供服務， 其中每個企業都需要其自己的組織。

ISP 可支援數以百萬計需要郵件服務的一般使用者。而且，ISP 還可與管理一般使用者業務的協力廠商經銷商合作。

每天都有許多新的組織應增加至目錄中。

在兩階式階層中，TLA 應建立所有這些新組織。

在三階式階層中，管理作業委託給第二層級的管理員。此第二層級的委託可使對大型 LDAP 目錄支援的大型用戶基底的管理變得容易。

爲支援此階層，Delegated Administrator 推出一個新角色，即服務提供者管理員 (SPA)。

SPA 的權限範圍介於頂層管理員 (TLA) 和組織管理員 (OA) 的權限之間。

圖 1–3 顯示了三階式階層中管理員角色範例。

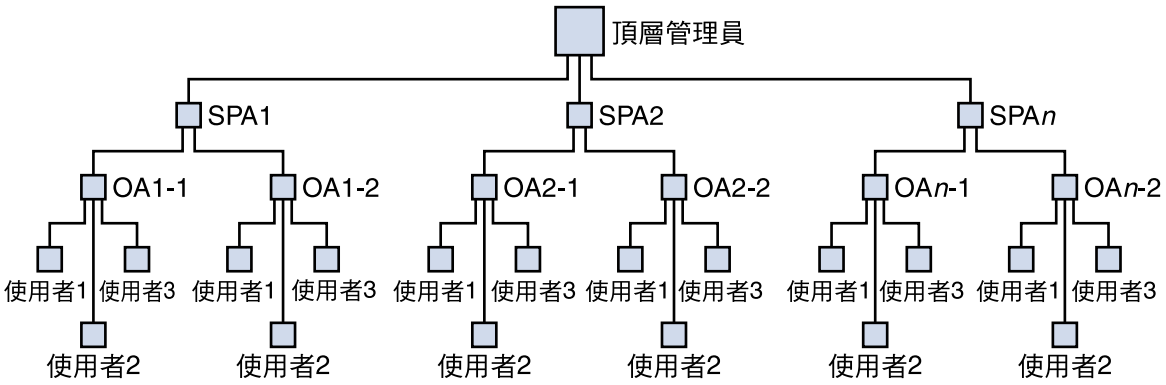

圖 1–3 三階式階層中的管理員角色

在三階式階層中，TLA 將管理權限委託給服務提供者管理員 (SPA)。SPA 可以爲新用戶建立從屬組織，並指定組織管理員 (OA) 以管理這些組織中的使用者。

如果您需要其自身分爲多個子群組或組織的多個組織，則可使用可實作 TLA、SPA 和 OA 角色的三階式階層。

如需有關 SPA 角色的資訊，請參閱附錄 A。

管理員角色和目錄階層

本小節顯示可實作一階式和兩階式階層的目錄資訊樹狀結構範例。然後說明可由頂層管理員和組織管理員執行的作業。

支援一階式階層的目錄結構

透過執行配置程式 `config-commda` 配置 Delegated Administrator 時，可建立頂層管理員 (TLA) 和預設組織。

一階式階層：根字尾下的預設組織

依預設，配置程式將預設組織放置於根字尾下。

目錄資訊樹狀結構類似於圖 1–4 中顯示的樹狀結構。

圖 1–4 顯示了以一階式階層組織 (預設配置) 的目錄資訊樹狀結構範例。

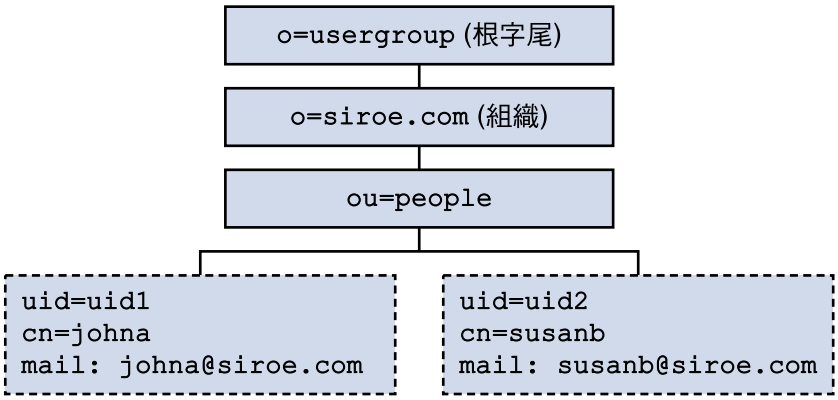

圖 1–4 一階式階層：目錄資訊樹狀結構 (預設) 範例

一階式階層：根字尾處的預設組織

執行配置程式 `config-commda` 時，您可以選擇在根字尾處 (而非在其下) 建立預設組織。如需配置詳細資訊，請參閱第 3 章中的第 63 頁的 「配置 Delegated Administrator 伺服器」。

在此情況下，目錄資訊樹狀結構將類似於圖 1–5 中顯示的樹狀結構。

但是，如果您在根字尾處建立預設組織，則此 LDAP 目錄配置將無法支援多個託管網域。若要支援託管網域，預設組織必須位於根字尾下。

圖 1–5 顯示了在根字尾處建立預設組織的一階式階層範例。

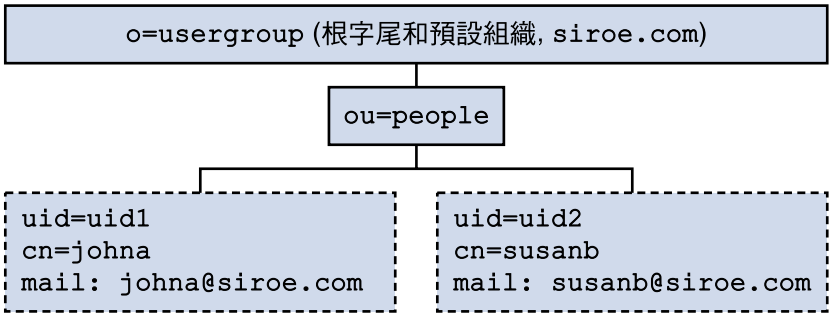

圖 1–5 一階式階層：根字尾處的預設組織

支援兩階式階層的目錄結構

使用 `config-commda` 程式配置 Delegated Administrator 之後，TLA 可以建立其他組織，如圖 1–6 中所示。

圖 1–6 顯示了以兩階式階層組織的目錄資訊樹狀結構範例。

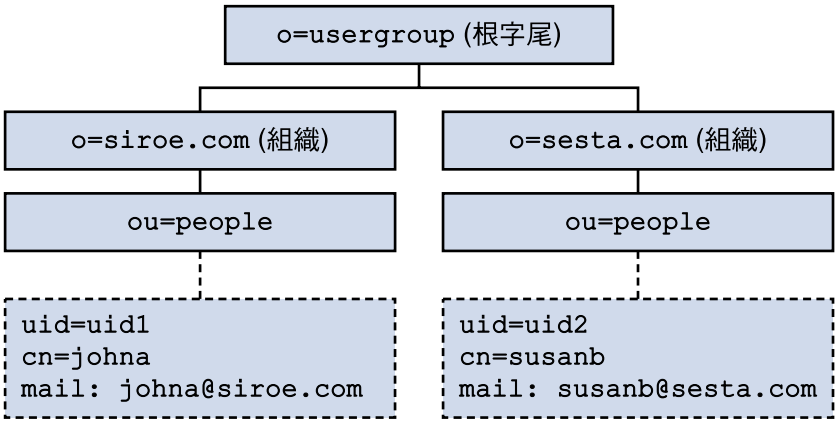

圖 1–6 兩階式階層：目錄資訊樹狀結構範例

頂層管理員角色

TLA 具有執行以下作業的權限：

- 建立、刪除和修改組織。

  在圖 1–6 所示的範例中，TLA 可以修改或刪除 `siroe.com` 或 `sesta.com`，以及建立其他組織。

  請注意，此範例中的兩個組織也是唯一 (託管) 網域。
- 建立、刪除和修改使用者。
- 建立、刪除和修改群組。
- 建立、刪除和修改行事曆資源。
- 將 OA 角色指定給使用者。例如，TLA 可以將 OA 角色指定給 `siroe.com` 組織中的使用者 `johna`。

  TLA 也可以移除使用者的 OA 角色。
- 將 TLA 角色指定給其他使用者。TLA 也可以移除使用者的 TLA 角色。
- 爲組織指定服務套裝軟體。

  如需有關服務套裝軟體的資訊，請參閱本簡介後面部分的第 30 頁的 「服務套裝軟體」。

TLA 可以爲組織指定特定類型的服務套裝軟體，並確定該組織中可以使用的每種套裝軟體的最大數目。

例如，TLA 可以指定以下服務套裝軟體：

- 在 `siroe.com` 組織中：

  `1,000 gold packages`

  `500 platinum packages`
- 在 `sesta.com` 組織中：

  `2,000 silver packages`

  `1,500 gold packages`

  `100 platinum packages`

  TLA 可以透過使用 Delegated Administrator 主控台或執行 Delegated Administrator 公用程式 (`commadmin`) 指令來執行前面的作業。

  如需 `commadmin` 指令的說明，請參閱第 5 章中的表 5–1。

組織管理員角色

OA 具有在其組織中執行以下作業的權限：

- 建立、刪除和修改使用者。

  在圖 1–6 所示的範例中，如果將 `siroe.com` 組織中的 OA 角色指定給使用者 `johna`，則 `johna` 可管理 `siroe.com` 中的使用者。
- 建立、刪除和修改群組。
- 建立、刪除和修改行事曆資源。
- 將 OA 角色指定給其他使用者。
- 指定與移除使用者的服務套裝軟體。

OA 無法對其組織之外的使用者、群組或資源執行這些作業中的任何作業。

例如，如果 `johna` 是圖 1–6 中 `siroe.com` 的 OA，則 `johna` 無法管理 `sesta.com` 中的使用者、群組或資源。

OA 可以透過使用 Delegated Administrator 主控台或執行 Delegated Administrator 公用程式 (`commadmin`) 指令來執行前面的作業。

如需可供 OA 使用的 `commadmin` 指令的說明，請參閱第 5 章中的表 5–1。

對於 iPlanet Delegated Administrator 的前使用者

Communications Services Delegated Administrator 專用於在 LDAP Schema 2 目錄中佈建使用者。

具有 LDAP Schema 1 目錄的之前版本之 Messaging Server 的使用者可能已使用 iPlanet Delegated Administrator (一個已停用的工具)。如果您仍具有 Schema 1 目錄，則應使用 iPlanet Delegated Administrator 佈建使用者。

iPlanet Delegated Administrator 使用的管理員角色術語與 Communications Service Delegated Administrator 目前使用的管理員角色術語稍有不同。

表 1–1 列出並定義了每個 Delegated Administrator 版本中的管理員角色。

表 1–1 iPlanet Delegated Administrator 和 Communications Services Delegated Administrator 中的管理員角色

iPlanet Delegated Administrator	Communications Services Delegated Administrator 公用程式	Communications Services Delegated Administrator 主控台	定義
網站管理員	頂層管理員 (TLA)	頂層管理員 (TLA)	管理 Delegated Administrator 支援的整個目錄，包括組織和使用者 *。
(無)	(此發行版本中不存在)	服務提供者管理員 (SPA)	管理提供者組織、提供者組織下的共用和完整商務組織，以及這些商務組織中的使用者。
網域管理員	組織管理員 (OA)	組織管理員 (OA)	管理一個組織和該組織中的使用者。
* 在此發行版本的 Delegated Administrator 中，TLA 無法在提供者組織下建立提供者組織或商務組織。			

服務套裝軟體

服務套裝軟體在 LDAP 目錄中由服務類別機制實作。此機制可讓您在配置 Delegated Administrator 時，爲安裝在目錄中的預先定義之屬性進行值的設定。服務套裝軟體可將服務特徵增加至使用者或群組項目。

Delegated Administrator 可提供服務類別範本範例。

您也可以建立自己的服務套裝軟體。

在 Delegated Administrator 主控台中，您可以將套裝軟體範例和您自己的套裝軟體指定給使用者或群組。

服務套裝軟體的類型

服務套裝軟體包括以下元件：

- Access Manager 服務
- 服務束 (郵件服務和/或行事曆服務)
- LDAP 物件 (使用者或群組)

Delegated Administrator 自動提供 Access Manager 服務以及每種服務定義。將服務套裝軟體指定給使用者或群組時，Delegated Administrator 會從服務定義中擷取 Access Manager 物件類別和屬性，並將它們增加至 LDAP 項目。

請勿變更或刪除任何服務套裝軟體的 Access Manager 部分。

建立服務套裝軟體時，您可以配置其服務束和 LDAP 物件。

服務束

Delegated Administrator 提供兩種類型的服務：郵件服務和行事曆服務。

服務套裝軟體隨附一種或多種服務，以及與服務相關的屬性集。因此，個別服務套裝軟體可能包含以下服務組合：

- 僅郵件服務
- 僅行事曆服務
- 郵件和行事曆服務

備註 – 僅郵件服務在其服務類別定義中具有 LDAP 屬性。行事曆服務沒有與之相關的屬性。

爲特定 LDAP 物件定義的套裝軟體

服務套裝軟體是爲使用者或群組定義的。您無法將同一服務套裝軟體同時指定給使用者和群組。

Delegated Administrator 可提供具有以下服務束和 LDAP 物件的服務套裝軟體：

- 使用者郵件服務
- 使用者行事曆服務
- 使用者郵件和行事曆服務
- 群組郵件服務

備註 – 僅郵件服務可以指定給群組。在此發行版本的 Delegated Administrator 中，群組無法具有行事曆服務。

關於群組

在 Delegated Administrator 中，群組爲 LDAP 目錄中包含使用者清單的項目。群組特徵不會傳送至是其成員的使用者。例如，將服務套裝軟體指定給群組時，是該群組成員的使用者不會繼承服務套裝軟體屬性。

將郵件服務套裝軟體指定給群組後，該群組將成爲由 Messaging Server 使用的郵件收信人清單。

Delegated Administrator 提供的服務套裝軟體

配置 Delegated Administrator 時，您可以選擇安裝一組預先定義的服務類別範本範例。Delegated Administrator 主控台將顯示這些範本。

(執行配置程式時，選取 [**服務套裝軟體和組織範例**] 面板中的 [**載入服務套裝軟體範例**]。)配置程式可將 `cos.sample.ldif` 檔案增加至 LDAP 目錄。

您可以使用範本範例爲使用者和群組提供服務和郵件屬性。如需範本及其屬性值的清單，請參閱第 35 頁的 「服務類別範本範例」。

圖 1–7 顯示了使用者服務套裝軟體範本。

圖 1–7 [所有使用者服務套裝軟體] 頁面 — 顯示範本範例

圖 1–8 顯示了群組服務套裝軟體範本。

圖 1–8 [所有群組服務套裝軟體] 頁面 — 顯示範本範例

服務套裝軟體作業

在 Delegated Administrator 主控台中，您可以執行以下服務套裝軟體作業：

- 將服務套裝軟體配置給組織。透過將一些 (或全部) 套裝軟體配置給組織，使該組織中的使用者或群組可以使用這些套裝軟體。

  對於每個套裝軟體，您可以配置指定數目的套裝軟體。

  例如，對 ABC 組織，您可以配置 5,000 個黃金服務套裝軟體、10,000 個金星服務套裝軟體 和 500 個大西洋服務套裝軟體。
- 將服務套裝軟體指定給使用者。
- 將服務套裝軟體指定給群組。

指定服務套裝軟體的準則

- 配置給組織的服務套裝軟體組成池，可以從該池中將服務套裝軟體指定給組織中的使用者或群組。
- 您可以將多個服務套裝軟體指定給使用者或群組。
- 將服務套裝軟體指定給使用者或群組時，該服務套裝軟體中的所有屬性和值都會被自動指定給該使用者或群組。
- 若要僅將行事曆服務指定給使用者，請使用 standardUserCalendar 服務套裝軟體。行事曆服務沒有任何關聯屬性。

  指定 standardUserCalendar 服務套裝軟體等同於使用 `commadmin user create` 或 `commadmin user modify` 指令中的 `-s cal` 選項。

如需有關如何配置和指定服務套裝軟體的說明，請參閱 Delegated Administrator 主控台線上說明。

建立您自己的服務套裝軟體

本章中所述的服務類別範本僅做爲範例。很多時候，您可能希望建立自己的服務套裝軟體，其屬性值適用於您的安裝中的使用者和群組。

若要建立您自己的服務套裝軟體，可以使用儲存在 `da.cos.skeleton.ldif` 檔案中的服務類別範本。此檔案專爲用做用於寫入服務套裝軟體的範本而建立。配置 Delegated Administrator 時，此檔案未安裝在 LDAP 目錄中。

您可以複製和編輯 `da.cos.skeleton.ldif` 檔案，並使用 LDAP 目錄工具 (如 `ldapmodify`) 在目錄中安裝自訂的服務類別範本。

Delegated Administrator 主控台可顯示您自訂的範本和範本範例。在主控台中，服務類別範本稱爲服務套裝軟體。當您可以將服務套裝軟體指定給使用者或群組時，Delegated Administrator 會寫入使用者或群組 LDAP 項目和完整的服務套裝軟體，包括 Access Manager 服務。

如需有關使用 `da.cos.skeleton.ldif` 檔案配置您自己的服務套裝軟體的說明，請參閱第 3 章中的第 70 頁的 「建立服務套裝軟體」。

檢視延伸式服務套裝軟體的限制

您可以透過向定義項目增加屬性，來延伸 Delegated Administrator 服務套裝軟體定義。

但是，在此發行版本的 Delegated Administrator 中，主控台僅可讓您檢視配置 Delegated Administrator 時提供的預先定義的屬性。Delegated Administrator 主控台不會顯示您增加至服務套裝軟體定義中的任何屬性。

在此發行版本中，您也不應從 Delegated Administrator 提供的服務類別定義中移除預先定義的屬性定義。

指定給 LDAP 項目的服務套裝軟體範例

使用 Delegated Administrator 將服務套裝軟體指定給使用者或群組時，單一屬性 (inetCOS) 會被增加至 LDAP 目錄中的使用者或群組項目中。inetCOS 屬性的值可將整個服務套裝軟體指定給使用者或群組，包括服務及與該服務相關的所有屬性。(inetCOS 爲多值屬性。)

例如，假設您將白金套裝軟體指定給使用者。以下屬性會被增加至使用者項目：

```
inetCOS: platinum
```

白金套裝軟體可爲使用者提供郵件服務。該套裝軟體還包含以下郵件屬性值。因此，指定白金套裝軟體可將以下屬性增加至使用者項目：

```
mailMsgMaxBlocks: 800
mailQuota: 10000000
mailMsgQuota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
```

Access Manager 服務定義可提供郵件和/或行事曆服務所需的物件類別和屬性。指定服務套裝軟體時，Delegated Administrator 會將這些物件類別和屬性增加至使用者或群組項目中。

服務類別範本範例

本小節列出了服務類別範本範例以及該範本提供的郵件屬性值。

這些範本包含在 cos.sample.ldif 檔案中。

郵件服務屬性

郵件服務包含爲郵件使用者定義的 LDAP 屬性。表 1–2 定義了這些屬性。

表 1–2 可以在服務套裝軟體中使用的郵件服務屬性

屬性	定義
mailMsgMaxBlocks	可傳送給使用者或群組的最大郵件大小，以 MTA 區段爲單位。
mailAllowedServiceAccess	指定可存取指定服務的可用用戶端的篩選器。例如：+imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
mailMsgQuota	使用者可使用的郵件最大數目 (包括所有使用者資料夾)。
mailQuota	使用者的電子信箱可使用的磁碟空間 (以位元組爲單位)。

如需有關這些屬性的更多資訊，請參閱「*Sun Java System Communications Services Schema Reference*」中的「Chapter 3: Messaging Server and Calendar Server Attributes」。

使用者郵件範本範例

白金

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

黃金

```
mailMsgMaxBlocks: 700
mailquota: 8000000
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

銀

```
mailMsgMaxBlocks: 300
mailquota: 6291456
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

銅

```
mailMsgMaxBlocks: 700
mailquota: 5242288
mailmsgquota: 3000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

紅寶石

```
mailMsgMaxBlocks: 600
mailquota: 1048576
mailmsgquota: 2000
mailAllowedServiceAccess: +pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

綠寶石

```
mailMsgMaxBlocks: 600
mailquota: 2097152
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

鑽石

```
mailMsgMaxBlocks: 5000
mailquota: 3145728
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

黃寶石

```
mailMsgMaxBlocks: 3000
mailquota: 4194304
mailmsgquota: 2000
mailAllowedServiceAccess: +imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

使用者行事曆範本範例

無 *(standardUserCalendar)*

沒有預先定義的服務類別範本，用於提供行事曆服務且包含屬性值。提供的行事曆服務沒有關聯屬性。

由於不存在範本範例，Delegated Administrator 會直接從使用者行事曆服務類別定義中產生預設服務套裝軟體 (沒有範本)。其名稱與服務類別定義的名稱相同，均爲：standardUserCalendar。

此服務套裝軟體僅提供行事曆服務。

使用者郵件和行事曆範本範例

以下範本範例適用於郵件服務和行事曆服務。

水銀

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
```

```
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

金星

```
mailMsgMaxBlocks: 700
mailquota: 8000000
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

地球

```
mailMsgMaxBlocks: 300
mailquota: 6291456
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

火星

```
mailMsgMaxBlocks: 700
mailquota: 5242288
mailmsgquota: 3000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

群組郵件範本範例

大西洋

```
mailMsgMaxBlocks: 800
daServiceType: mail group
```

太平洋

```
mailMsgMaxBlocks: 900
daServiceType: mail group
```

印度洋

```
mailMsgMaxBlocks: 1000
daServiceType: mail group
```

北極

```
mailMsgMaxBlocks: 1200
daServiceType: mail group
```

服務類別定義

此發行版本的 Delegated Administrator 提供了每種類型的服務套裝軟體的服務類別定義：

- 使用者郵件服務
- 使用者行事曆服務
- 使用者郵件和行事曆服務
- 群組郵件服務

配置 Delegated Administrator 時，會在目錄中安裝服務類別定義。

在每個定義中，`daServiceType` 屬性都使用以下語法確定服務套裝軟體的類型：

`daServiceType: <service type> <target>`

其中 *service type* 爲郵件服務、行事曆服務，或二者，*target* 爲使用者或群組。

使用者的郵件服務

使用者郵件服務在名爲 `standardUserMail` 的服務類別定義中定義：

```
#
#  Definition for user mail service bundle
#
dn: cn=standardUserMail,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mailAllowedServiceAccess
cosAttribute: mailMsgMaxBlocks
cosAttribute: mailquota
cosAttribute: mailmsgquota
daServiceType: mail user


NOTE: When the Delegated Administrator configuration program installs the
standardUserMail definition in the directory, the variable
<ugldapbasedn>, shown above, is replaced by your root suffix
(such as o=usergroup).
```

daServiceType 屬性將此定義爲使用者的郵件服務。

使用者的行事曆服務

使用者行事曆服務在名爲 standardUserCalendar 的服務類別定義中定義：

```
#
#  Definition for user calendar service bundle
#
dn: cn=standardUserCalendar,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: icsPreferredHost
cosAttribute: icsDWPHost
cosAttribute: icsFirstDay
daServiceType: calendar user


NOTE: When the Delegated Administrator configuration program installs the
standardUserCalendar definition in the directory, the variable
<ugldapbasedn>, shown above, is replaced by your root suffix
(such as o=usergroup).
```

daServiceType 屬性將此定義爲使用者的行事曆服務。

備註 – 請注意，行事曆服務定義還包含行事曆屬性，如 icsPreferredHost。

但是，Delegated Administrator 未提供可爲這些屬性指定值的服務套裝軟體範本。Delegated Administrator 主控台提供一個僅具有行事曆服務的服務套裝軟體：standardUserCalendar 服務套裝軟體。此套裝軟體不包含行事曆屬性。

使用者的郵件服務和行事曆服務

使用者郵件服務和行事曆服務在名爲 standardUserMailCalendar 的服務類別定義中定義：

```
#
#  Definition for user mail and user calendar service bundle
#
dn: cn=standardUserMailCalendar,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
```

```
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: icsPreferredHost
cosAttribute: icsDWPHost
cosAttribute: icsFirstDay
cosAttribute: icsQuota
cosAttribute: mailAllowedServiceAccess
cosAttribute: mailMsgMaxBlocks
cosAttribute: mailquota
cosAttribute: mailmsgquota
daServiceType: calendar user
daServiceType: mail user
```

```
NOTE: When the Delegated Administrator configuration program installs the
standardUserMailCalendar definition in the directory, the variable
<ugldapbasedn>, shown above, is replaced by your root suffix
(such as o=usergroup).
```

兩個 daServiceType 屬性項目將此定義爲使用者的行事曆服務和郵件服務。

群組的郵件服務

群組郵件服務在名爲 standardGroupMail 的服務類別定義中定義：

```
#
#  Definition for group mail service bundle
#
dn: cn=standardGroupMail,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mailMsgMaxBlocks
daServiceType: mail group
```

```
NOTE: When the Delegated Administrator configuration program installs the
standardGroupMail definition in the directory, the variable <ugldapbasedn>,
shown above, is replaced by your root suffix (such as o=usergroup).
```

daServiceType 屬性將此定義爲群組的郵件服務。

服務類別定義和套裝軟體的位置

在 LDAP 目錄資訊樹狀結構 (DIT) 中，服務類別定義位於緊跟在根字尾之下的節點中。由於服務套裝軟體儲存在 DIT 的頂層，所以可以將它們指定給目錄中的所有使用者項目。

圖 1–9 顯示了服務定義和套裝軟體在 DIT 中的位置。

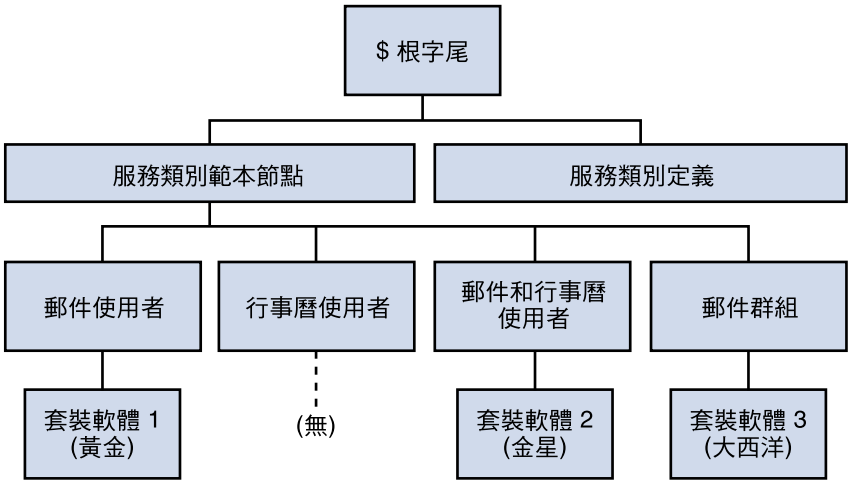

圖 1–9 服務類別定義和套裝軟體在目錄樹狀結構中的位置

每種類型的服務類別範本都位於其自己的節點之下。因此，爲使用者提供郵件服務的範本位於郵件使用者節點之下。此結構可讓 Delegated Administrator 在向使用者或群組指定服務套裝軟體時，使用正確的服務類別定義 (如 `standardUserMail`)。

Delegated Administrator 使用傳統型服務類別定義。

如需有關服務類別機制的更多資訊，請參閱「*Sun Java System Directory Server Administration Guide*」。特別是「第 5 章：管理身分和角色」中的「定義服務類別 (CoS)」。

「*Sun Java System Directory Server Administration Guide*」還說明相關主題，例如在指定給使用者的服務套裝軟體中定義的屬性已存在於該個別使用者項目中時，決定優先考量哪個服務屬性值。

第 2 章

安裝與配置規劃

若要在 Solaris 系統上安裝 Sun Java System Communications Services Delegated Administrator，您必須使用 Sun Java Enterprise System 安裝程式，此程式也可安裝其他 Sun 元件產品。

若要安裝和配置 Delegated Administrator，請依照以下步驟執行：

1. 第 43 頁的 「收集 Delegated Administrator 配置資訊」
2. 第 47 頁的 「執行 Java Enterprise System 安裝程式」
3. 第 48 頁的 「執行 Directory Server 設定程序檔」
4. 第 48 頁的 「配置 Delegated Administrator」
5. 第 49 頁的 「配置 Messaging Server 和 Calendar Server」

   如需有關 Delegated Administrator 的最新資訊，請參閱「Sun Java System Communications Services Release Notes」。

收集 Delegated Administrator 配置資訊

Delegated Administrator 元件

Delegated Administrator 由以下元件組成：

- **Delegated Administrator 公用程式 (用戶端)** — 使用 `commadmin` 呼叫的指令行介面。

  必需。您必須在安裝 Delegated Administrator 的所有機器上配置此公用程式。
- **Delegated Administrator 伺服器** — 執行 Delegated Administrator 公用程式和主控台所需的 Delegated Administrator 伺服器元件。

必需。您必須在至少一台機器上配置 Delegated Administrator 伺服器。

- **Delegated Administrator 主控台** — Delegated Administrator 圖形化使用者介面 (GUI)。

  選擇性的。如果您想僅使用 Delegated Administrator 公用程式，則不必配置主控台。

Web 容器

另外，必須將 Delegated Administrator 伺服器和主控台部署至 Web 容器。您可以在以下 Web 容器上配置 Delegated Administrator 主控台和伺服器

- Sun Java System Web Server
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

請遵循以下準則：

- Delegated Administrator 伺服器必須部署至 Access Manager 使用的 Web 容器。
- 您可以在兩個不同的 Web 容器上、兩個不同的 Web 容器實例上，或同一 Web 容器上部署 Delegated Administrator 主控台和伺服器。

配置資訊

在配置 Delegated Administrator 之前，您應收集配置資訊。

表 2–1 列出了 Delegated Administrator 所需的配置選項。

表 2–2 列出了用於在 Web 伺服器上進行部署的配置選項。

表 2–3 列出了用於在 Application Server 7.*x* 上進行部署的配置選項。

表 2–4 列出了用於在 Application Server 8.*x* 上進行部署的配置選項。

表 2–1 Delegated Administrator：必需的配置選項

選項	說明
配置目錄	儲存配置檔案和資料檔的目錄。
Access Manager 主機名稱	安裝 Access Manager 的主機名稱。Delegated Administrator 伺服器應安裝在同一伺服器上。
Access Manager 連接埠號	Access Manager 的連接埠號。應與 Web Server 連接埠號相同。
預設網域	頂層管理員的預設網域。如果在執行 `commadmin` 指令行公用程式時 `-n` 選項未明確指定網域，則使用此網域。

表 2–1 Delegated Administrator：必需的配置選項　*(續)*

選項	說明
預設 SSL 連接埠	Delegated Administrator 用戶端使用的 SSL 連接埠。
Access Manager 基底目錄	安裝 Access Manager 的目錄。預設目錄爲 `/opt/SUNWam`。
LDAP URL	使用者和群組目錄伺服器 LDAP URL。
連結爲	使用者和群組目錄伺服器目錄管理員。例如「cn=Directory Manager」。
LDAP 密碼	使用者和群組目錄管理員密碼。
Access Manager 頂層管理員使用者 ID 和密碼	Access Manager 頂層管理員的使用者 ID 和密碼
Access Manager 內部 LDAP 認證使用者的密碼	Access Manager 建立的使用者。此爲 LDAP 服務的 BindDN 使用者。
組織名稱	用於命名 LDAP 子樹狀結構，其下包含屬於預設電子郵件網域的所有電子郵件使用者和群組。
預設組織之頂層管理員的使用者 ID 和密碼	將在預設組織中建立的頂層管理員的使用者 ID 和密碼。
組織範例的喜好郵件主機	安裝 Messaging Server 之機器的名稱。如果您選擇在目錄中安裝組織範例，則必須輸入喜好的郵件主機。

表 2–2 Web Server 配置選項

選項	說明
Web Server 根 (實例) 目錄	Web Server 實例所在的目錄。Web Server 實例檔案儲存在 Web Server 安裝目錄下的 `https-`*host*`.`*domain* 目錄中。
Web Server 實例識別碼	Web Server 實例的完全合格的網域名稱。這可由 *host.domain* 名稱 (如 west.sesta.com) 指定。
虛擬伺服器識別碼	由 `https-`*host.domain* 名稱 (如 `https-west.sesta.com`) 指定。
HTTP 連接埠號	Web Server 的 HTTP 連接埠號。

表 2–3 Application Server 7.*x* 配置選項

選項	說明
Application Server 安裝目錄	安裝 Application Server 7.*x* 的目錄。依預設，此目錄爲 `/opt/SUNWappserver7`。
Application Server 網域目錄	依預設，此目錄爲 `/var/opt/SUNWappserver7/domains/domain1`。

表 2–3 Application Server 7.*x* 配置選項　*(續)*

選項	說明
Application Server 文件根目錄	依預設，此目錄爲 `/var/opt/SUNWappserver7/ \ domains/domain1/server1/docroot`
Application Server 實例名稱	實例名稱。例如：`server1`。
虛擬伺服器識別碼	Application Server 虛擬伺服器識別碼的名稱。例如：`server1`。
Application Server 實例 HTTP 連接埠號	Application Server 實例的 HTTP 連接埠號。
Administration Server 連接埠號	Application Server 7.*x* 之 Administration Server 實例的連接埠號。例如：`4848`。
Administration Server 管理員使用者 ID 和密碼。	Administration Server 管理員的使用者 ID 和密碼。使用者 ID 範例：`admin`
對 Administration Server 實例的 HTTP 或 HTTPS 存取	您需要指定對 Administration Server 實例的 HTTP 存取是否安全。

表 2–4 Application Server 8.*x* 配置選項

選項	說明
Application Server 安裝目錄	安裝 Application Server 8.*x* 的目錄。依預設，此目錄爲 `/opt/SUNWappserver/appserver`。
Application Server 網域目錄	依預設，此目錄爲 `/var/opt/SUNWappserver/domains/domain1`。
Application Server 文件根目錄	依預設，此目錄爲 `/var/opt/SUNWappserver/domains/domain1/docroot`
Application Server 目標名稱	實例名稱。例如：`server`。
虛擬伺服器識別碼	Application Server 虛擬伺服器識別碼的名稱。例如：`server`。
Application Server 目標 HTTP 連接埠號	Application Server 目標的 HTTP 連接埠號。
Administration Server 連接埠號	Application Server 8.*x* 之 Administration Server 實例的連接埠號。例如：`4849`。
Administration Server 管理員使用者 ID 和密碼。	Administration Server 管理員的使用者 ID 和密碼。使用者 ID 範例：`admin`
對 Administration Server 實例的 HTTP 或 HTTPS 存取	您需要指定對 Administration Server 實例的 HTTP 存取是否安全。

執行 Java Enterprise System 安裝程式

Java Enterprise System 安裝程式可安裝一系列互通的產品、共用元件和程式庫。

若要成功安裝和配置 Delegated Administrator，您需要執行 Java Enterprise System 安裝程式來安裝以下元件：

- Sun Java System Directory Server 5.x
- Sun Java System Access Manager 7.0

  Access Manager 7 有兩種安裝類型：Legacy 模式 (預設) 和 Realm 模式。Legacy 模式與 Delegated Administrator 相容。

  執行 Java Enterprise System 安裝程式時，必須在第一個 Access Manager 面板中選擇 Legacy 模式做爲安裝類型。請勿選擇 Realm 模式。

  由於 Delegated Administrator 需要您使用 LDAP Schema 2 佈建使用者和群組，所以需要安裝 Access Manager。
- 以下 Web 容器之一：
  - Sun Java System Web Server 6.1
  - Sun Java System Application Server 7.*x*
  - Sun Java System Application Server 8.*x*

    (Java Enterprise System 安裝程式還會檢查以確保您已安裝 Directory Server 5.x 和以上列出的 Web 容器之一。)
- Sun Java System Messaging Server 和 Sun Java System Calendar Server 之一或二者。

  Delegated Administrator 是 Messaging Server 和 Calendar Server 的佈建工具。因此，若要成功使用 Delegated Administrator，您應安裝這兩個應用程式之一或二者都安裝。

  請參閱「Sun Java System Messaging Server Administration Guide」以獲得有關配置 Messaging Server 的說明。請參閱「Sun Java System Calendar Server Administration Guide」以獲得有關配置 Calendar Server 的說明。
- Delegated Administrator

  Java Enterprise System 安裝程式中的某個面板會詢問是否要安裝 Delegated Administrator。在此面板中，指定您要安裝 Delegated Administrator。

  (在舊的發行版本中，Delegated Administrator 自動與 Access Manager 一起安裝。)

  安裝程式將 Delegated Administrator 安裝在稱爲 *da_base* 的目錄中 (例如，預設爲 `/opt/SUNWcomm`)。

如需有關 Java Enterprise System 安裝程式的資訊，請參閱「Sun Java Enterprise System Installation Guide」。

備註 – 如果您要從之前的 Sun Java System 版本升級 Delegated Administrator，請參閱「Sun Java Enterprise System Upgrade and Migration Guide」中名爲「Upgrading Delegated Administrator」的章節。

執行 Directory Server 設定程序檔

在配置 Delegated Administrator 之前，必須執行 Messaging Server、Calendar Server 或 Directory Server 準備工具程序檔 (`comm_dssetup.pl`)。您只需執行一次 `comm_dssetup.pl` 程序檔。

此程序檔將 LDAP 目錄伺服器配置爲與 Delegated Administrator、Messaging Server 或 Calendar Server 配置配合工作。`comm_dssetup.pl` 程序檔透過設定新模式、索引及配置資料來準備 Directory Server。

請參閱「Sun Java System Messaging Server Administration Guide」或「Sun Java System Calendar Server Administration Guide」，以獲得 `comm_dssetup.pl` 程序檔的說明和選項。

若要執行 Delegated Administrator，您必須在執行 `comm_dssetup.pl` 程序檔時選取「Schema 2」模式類型。

合併目錄中的 ACI

若要大規模安裝 Access Manager、Messaging Server 以及 LDAP Schema 2 目錄，您可能需要合併目錄中的存取控制指令 (ACI)。

安裝 Messaging Server 和 Access Manager 時，目錄中初始即已安裝大量的 ACI。Messaging Server 不需要或不使用許多預設 ACI。您可以透過合併並減少目錄中的預設 ACI 數目來提高 Directory Server 的效能，然後提高 Messaging Server 查詢的效能。

如需有關如何合併和捨棄未使用的 ACI 的資訊，請參閱本指南的後面部分附錄 E。

配置 Delegated Administrator

安裝 Delegated Administrator 後，請使用第 43 頁的 「收集 Delegated Administrator 配置資訊」中的資訊執行 Delegated Administrator 配置程式

如需有關執行配置程式的資訊，請參閱第 3 章。

配置 Messaging Server 和 Calendar Server

請參閱「Sun Java System Messaging Server Administration Guide」以獲得有關配置 Messaging Server 的說明。請參閱「Sun Java System Calendar Server Administration Guide」以獲得有關配置 Calendar Server 的說明。

第 3 章

配置 Delegated Administrator

Delegated Administrator 配置程式 (`config-commda`) 可根據您的特定需求建立新配置。此初始執行階段配置程式會執行最小配置。

執行此程式後，請按照第 69 頁的 「配置後作業」中所述的步驟完成初始配置。

您可以透過執行第 4 章中所述的作業，進一步自訂 Delegated Administrator 配置。

您可能需要執行其他配置，如「Sun Java System Messaging Server Administration Guide」中所述。

本章說明以下主題：

如果您要從之前發行版本的 Delegated Administrator 升級

如果您是首次配置 Delegated Administrator，則可略過本小節直接進入第 54 頁的 「選擇要配置的元件」小節。

如果您要從舊的 Java Enterprise System 發行版本升級至此 Delegated Administrator 發行版本，則可能需要在配置 Delegated Administrator 之前執行以下作業：

如需有關如何將 Delegated Administrator 從之前的 Sun Java System 版本升級的說明，請參閱「Sun Java Enterprise System Upgrade Guide」中名爲「Upgrading Delegated Administrator」的章節。

保留現有配置

僅當您之前已安裝和配置 Delegated Administrator 並且已自訂 Delegated Administrator 配置時，才需要參閱本小節。

如果您已自訂配置，則當您重新執行 Delegated Administrator 配置程式 `config-commda`，配置檔案中的特性會重設爲其預設值。這些檔案在下面的第 52 頁的「Delegated Administrator 特性檔案」中列出。

如需有關如何自訂 Delegated Administrator 的資訊，請參閱第 4 章。

您應該在升級 Delegated Administrator 之前保留自訂配置，或重新執行 Delegated Administrator 配置程式 (出於其他任何原因)。

Delegated Administrator 特性檔案

Delegated Administrator 可安裝以下特性檔案：

- `resource.properties`

  預設位置：

  da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet`
- `daconfig.properties`

  預設位置：

  da_base`/data/WEB-INF/classes/com/sun/comm/da/resources`
- `cli-usrprefs.properties`

  預設位置：`/var/opt/SUNWcomm/config`
- `security.properties`

  預設位置：*da_base*`/data/da/WEB-INF/classes/com/sun/comm/da/resources`
- `Resources.properties`

  預設位置：

  da_base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`
- `logger.properties`

  預設位置：

  da_base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`

▼ 保留現有配置

步驟 **1. 備份您已自訂的特性檔案。**

如需特性檔案及其預設位置的清單，請參閱第 52 頁的 「Delegated Administrator 特性檔案」。

2. 執行 `config-commda` 程式，如以下小節中所述。

剩餘步驟使用 `resource.properties` 檔案做爲範例。對您已自訂的每個檔案重複執行這些步驟。

3. 編輯 `config-commda` 程式建立的新 `resource.properties` 檔案，如下所示：

a. 開啓新的 `resource.properties` 檔案。

b. 開啓 `resource.properties` 檔案的備份副本。

c. 尋找在備份副本中自訂的特性。將自訂值套用至新的 `resource.properties` 檔案中的相應特性。

請勿簡單地使用整個備份副本覆寫新的 `resource.properties` 檔案。新檔案可能包含爲支援此發行版本的 Delegated Administrator 而建立的新特性。

升級自訂服務套裝軟體

僅當您要從 Communications Services 6 2005Q1 Delegated Administrator 升級至 Communications Services 6 2005Q4 Delegated Administrator，並且已在之前的發行版本 (6 2005Q1) 中建立自訂服務套裝軟體時，才需要參閱本小節。

在 Delegated Administrator 的目前發行版本 (6 2005Q4) 中，服務套裝軟體可以爲使用者或群組提供行事曆服務和郵件服務。在之前的發行版本 (6 2005Q1) 中，服務套裝軟體只爲使用者提供郵件服務。服務套裝軟體定義包含用於支援新功能的新屬性。

服務類別範本範例

執行 Delegated Administrator 配置程式時，之前透過 Delegated Administrator 配置程式安裝的服務類別範本範例會自動升級。(在配置程式中，應選取 **[服務套裝軟體和組織範例]** 面板中的 **[載入服務套裝軟體範例]**。)

如果您僅使用範本範例將服務套裝軟體指定給使用者和群組，則無需任何動作。

自訂服務套裝軟體

配置程式不會升級在 6 2005Q1 發行版本中建立的自訂服務套裝軟體。您必須手動升級自訂服務套裝軟體。

如需有關如何建立自訂服務套裝軟體的資訊，請參閱第 70 頁的 「建立您自己的服務套裝軟體」。

▼ 升級自訂服務套裝軟體

步驟 1. **透過將下行增加至定義服務套裝軟體的 ldif 檔案，來編輯每個自訂服務套裝軟體：**

```
daServiceType: mail user
```

`daServiceType` 屬性定義服務的類型 (郵件或行事曆) 及目標 (使用者或群組)。

在之前發行版本中建立的服務套裝軟體只爲使用者提供郵件服務。因此，`daServiceType` 的值應爲 `mail user`。

以下範例顯示了已編輯的 ldif 檔案：

```
dn: cn=myservicepackage,o=cosTemplates,o=mycompanysuffix
changetype: modify
replace: daServiceType
daServiceType: mail user
```

2. **使用 LDAP 目錄工具 `ldapmodify` 更新目錄中的服務套裝軟體。**
例如，您可以執行以下指令：

```
ldapmodify -D <directory manager> -w <password> -f
myservicepackage
```

其中，

`<directory manager>` 是 Directory Server 管理員的名稱。

`<password>` 是 Directory Service 管理員的密碼。

`myservicepackage` 是定義自訂服務套裝軟體的 ldif 檔案的名稱。

選擇要配置的元件

配置程式的第三個面板將會詢問您要配置哪些 Delegated Administrator 元件：

- **Delegated Administrator 公用程式 (用戶端)** — 使用 `commadmin` 呼叫的指令行介面。
- **Delegated Administrator 伺服器** — 執行 Delegated Administrator 公用程式和主控台所需的 Delegated Administrator 伺服器元件。
- **Delegated Administrator 主控台** — Delegated Administrator 圖形化使用者介面 (GUI)。

配置程式會根據您選取的元件顯示不同的面板。

以下步驟概括了配置選項。每個摘要步驟 (下面) 都會連結至可帶您進入實際配置面板的小節 (本章較後面的部分)。

▼ 配置選項摘要

步驟

1. **第 56 頁的 「啓動配置」**
   在這些面板中輸入所需資訊以開始配置。

2. **第 57 頁的 「配置 Delegated Administrator 公用程式」**
   這些面板緊跟在 **[選取要配置的元件]** 面板後面。它們要求用於配置 Delegated Administrator 公用程式的資訊。

   在安裝 Delegated Administrator 元件 (伺服器或主控台) 的所有機器上都必須安裝並配置 Delegated Administrator 公用程式。

   因此，您必須始終在這些面板中輸入資訊。

3. **第 58 頁的 「配置 Delegated Administrator 主控台」**
   這些面板在配置公用程式的面板之後。

   您可以選擇是否配置 Delegated Administrator 主控台。

   - 如果您在同一機器上部署 Delegated Administrator 主控台和伺服器，則應在 **[選取要配置的元件]** 面板中同時選取主控台和伺服器。
   - 您也可以在不同機器上部署 Delegated Administrator 主控台和伺服器。

     在您部署主控台的機器上，應在 **[選取要配置的元件]** 面板中僅選取主控台。(始終選取公用程式。)

     在此情況下，您必須在部署伺服器的機器上再次執行配置程式。

     如果您在不同機器上部署主控台和伺服器，則在**兩台**機器上都會配置公用程式。

   配置程式會根據您爲主控台選取的 Web 容器來顯示不同的面板。您可以部署至以下 Web 容器之一：

   - Sun Java System Web Server
   - Sun Java System Application Server 7.*x*
   - Sun Java System Application Server 8.*x*

   如果您要在一台機器上配置 Delegated Administrator 伺服器和主控台，您將需要按照這些說明執行**兩次** (一次爲伺服器，一次爲主控台)。

4. **第 63 頁的 「配置 Delegated Administrator 伺服器」**
   這些面板在配置主控台的面板之後。

   您可以選擇是否在給定的機器上配置 Delegated Administrator 伺服器。

如果您選擇不在給定的機器上配置伺服器，配置程式會警告您必須在其他機器上對其進行配置。伺服器元件是執行公用程式和主控台所必需的。

部署伺服器的所有其他注意事項與部署主控台的注意事項相同，如第 58 頁的 「配置 Delegated Administrator 主控台」中所述。

另請注意，伺服器與 Access Manager 使用相同的 Web 容器。(配置程式會在要求 Access Manager 基底目錄之後要求 Web 容器資訊。)

5. **第 65 頁的 「完成配置」**
   在這些面板中輸入所需資訊以完成配置。

執行配置程式

您可執行本小節中所述步驟來配置 Delegated Administrator。

啓動配置程式

若要執行配置程式，請以超級使用者身份登入 (或成爲超級使用者)，並至 `/opt/SUNWcomm/sbin` 目錄。然後輸入指令：

```
# ./config-commda
```

執行 `config-commda` 指令後，配置程式便會啓動。

接下來的小節將帶您進入配置面板。

啓動配置

您必須在第一個配置程式面板中輸入所需的資訊。

▼ 啓動配置

步驟 1. **歡迎使用**
   配置程式的第一個面板是版權頁面。按 **[下一步]** 以繼續，或按一下 **[取消]** 以結束。

2. **選取儲存配置檔案和資料檔的目錄**
   選取您要儲存 Delegated Administrator 配置檔案和資料檔的目錄。預設配置目錄爲 `/var/opt/SUNWcomm`。此目錄應與 *da_base* 目錄 (`/opt/SUNWcomm`) 分開。

輸入目錄的名稱，或保持預設，然後按 [**下一步**] 以繼續。

如果目錄不存在，螢幕上將顯示對話方塊，詢問您是要建立目錄還是選擇新目錄。按一下 [**建立目錄**] 以建立目錄，或按一下 [**選擇新目錄**] 以輸入新的目錄。

螢幕上將顯示對話方塊，指示正在載入元件。這個過程可能需要幾分鐘。

3. **選取要配置的元件**

   在 [元件] 面板中選取要配置的一個或多個元件。

   - **Delegated Administrator 公用程式 (用戶端)** — 使用 `commadmin` 呼叫的指令行介面。此元件是必要的，且依預設選取此元件。不能取消選取此元件。
   - **Delegated Administrator 伺服器** — 執行 Delegated Administrator 主控台所需的 Delegated Administrator 伺服器元件。
   - **Delegated Administrator 主控台** — Delegated Administrator 圖形化使用者介面 (GUI)。

   按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

   如需有關如何選擇元件的更多資訊，請參閱第 54 頁的 「選擇要配置的元件」

   如果您選擇不配置 Delegated Administrator 伺服器，螢幕上將顯示對話方塊，警告您必須在其他機器上配置 Delegated Administrator 伺服器。必須配置伺服器以使 Delegated Administrator 公用程式和主控台可以正常工作。

配置 Delegated Administrator 公用程式

您必須在安裝 Delegated Administrator 元件 (伺服器或主控台) 的所有機器上配置 Delegated Administrator 公用程式。

▼ 配置 Delegated Administrator 公用程式

步驟

1. **Access Manager 主機名稱和連接埠號**

   輸入 Access Manager (以前稱爲 Identity Server) 主機名稱和連接埠號。如果您要安裝 Delegated Administrator 伺服器元件，則必須將其與 Access Manager 安裝在同一主機上。

   按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

2. **預設網域**

   輸入頂層管理員的預設網域。如果在執行 `commadmin` 指令行公用程式時 `-n` 選項未明確指定網域，則使用此網域。此網域也做爲預設組織。如果目錄中不存在指定的網域，則會建立該網域。

   按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

3. **用戶端的預設 SSL 連接埠**

   輸入 Delegated Administrator 公用程式使用的預設 SSL 連接埠。

   按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

4. **如果您已選擇僅配置 Delegated Administrator 公用程式，請至**

   第 65 頁的 「完成配置」

   如果您已選擇同時配置 Delegated Administrator 主控台和伺服器，或已選擇僅配置主控台，請至

   第 58 頁的 「配置 Delegated Administrator 主控台」

   如果您已選擇僅配置 Delegated Administrator 伺服器 (連同所需的 Delegated Administrator 公用程式)，請至

   第 63 頁的 「配置 Delegated Administrator 伺服器」

配置 Delegated Administrator 主控台

現在，配置程式顯示以下面板：

為 Delegated Administrator 選取 Web 容器

選取您要在其上部署 Delegated Administrator 主控台的 Web 容器。您可以在以下 Web 容器上配置 Delegated Administrator

- Sun Java System Web Server
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

此面板以及後面的面板收集有關 Delegated Administrator 主控台的 Web 容器的資訊。依照相應小節中的說明執行：

- 第 59 頁的 「Web Server 配置」
- 第 60 頁的 「Application Server 7.*x* 配置 」
- 第 61 頁的 「Application Server 8.*x* 配置 」

您可以在兩個不同的 Web 容器上、兩個不同的 Web 容器實例上，或同一 Web 容器上部署 Delegated Administrator 主控台和伺服器。

如果您在面板 3 中選擇同時配置 Delegated Administrator 主控台和 Delegated Administrator 伺服器，將有另一系列的面板要求伺服器的 Web 容器資訊。

因此，您將看到 Web 容器配置面板兩次。依照部署每個 Delegated Administrator 元件的相應說明執行。

完成 Web 容器配置面板時：

- 如果您已選擇同時配置 Delegated Administrator 主控台和伺服器，請至
  第 63 頁的 「配置 Delegated Administrator 伺服器」
- 如果您已選擇僅配置 Delegated Administrator 主控台 (連同所需的 Delegated Administrator 公用程式)，請至
  第 65 頁的 「完成配置」

Web Server 配置

如果您要在 Web Server 上部署 Delegated Administrator 伺服器或主控台，請依照本小節中所述步驟執行。

▼ 配置 Web Server

步驟

1. **Web Server 配置詳細資訊**

   此面板文字告訴您是否要爲 Delegated Administrator 伺服器或主控台提供 Web Server 配置資訊。

   輸入 Web Server 根目錄。您可以瀏覽以選取目錄。

   輸入 Web Server 實例識別碼。這可由 *host.domain* 名稱 (如 `west.sesta.com`) 指定。

   輸入虛擬伺服器識別碼。這可由 `https-`*host.domain* 名稱 (如 `https-west.sesta.com`) 指定。

   如需有關 Web Server 實例識別碼和虛擬伺服器識別碼的更多資訊，請參閱 Web Server 文件。

   Web Server 實例的檔案儲存在 Web Server 安裝目錄下的 `https-`*host*`.`*domain* 目錄中，例如 `/opt/SUNWwbsvr/https-west.sesta.com`。

   輸入 Web Server 的 HTTP 連接埠號。

   按 **[下一步]** 以繼續，按 **[上一步]** 以返回前一個面板，或按一下 **[取消]** 以結束。

   配置程式會檢查您指定的值是否有效。如果目錄或識別碼無效或不存在，螢幕上將顯示對話方塊，告訴您選擇新的值。

   接下來，配置程式會檢查 Web Server 實例連線是否處於作用中。如果不是，螢幕上將顯示對話方塊，警告您配置程式無法連線至指定的實例，您的配置無法完成。您可以接受指定的值或選擇新的 Web Server 配置值。

2. **預設網域分隔符號**

   僅當您要配置 Delegated Administrator 主控台時，此面板才會顯示。網域分隔符號是配置主控台所必需的；此資訊與 Web 容器無關。

輸入使用者登入時要用於認證的預設網域分隔符號。例如：@。

網域分隔符號值包含在 daconfig.properties 檔案中。您可以在配置程式執行後編輯此特性值。如需更多資訊，請參閱第 4 章。

3. **如果您要配置 Delegated Administrator 主控台：**
   - 如果您已選擇同時配置 Delegated Administrator 主控台和伺服器，請至
     第 63 頁的 「配置 Delegated Administrator 伺服器」
   - 如果您已選擇僅配置 Delegated Administrator 主控台 (連同所需的 Delegated Administrator 公用程式)，請至
     第 65 頁的 「完成配置」

如果您要配置 Delegated Administrator 伺服器：

請至

第 63 頁的 「配置 Delegated Administrator 伺服器」中的步驟 3。

Application Server 7.*x* 配置

如果您要在 Application Server 7.*x* 上部署 Delegated Administrator 伺服器或主控台，請依照本小節中所述步驟執行。

▼ 配置 Application Server 7.*x*

步驟

1. **Application Server 7.x 配置詳細資訊**
   面板文字會告訴您是否要爲 Delegated Administrator 伺服器或主控台提供 Application Server 7.*x* 配置資訊。

   輸入 Application Server 安裝目錄。依預設，此目錄爲 /opt/SUNWappserver7。

   輸入 Application Server 網域目錄。依預設，此目錄爲 /var/opt/SUNWappserver7/domains/domain1。

   輸入 Application Server 文件根目錄。依預設，此目錄爲 /var/opt/SUNWappserver7/domains/domain1/server1/docroot。

   您可以瀏覽以選取這些目錄中的任何目錄。

   輸入 Application Server 實例名稱。例如：server1。

   輸入 Application Server 虛擬伺服器識別碼。例如：server1。

   輸入 Application Server 實例的 HTTP 連接埠號。

   按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

配置程式會檢查您指定的目錄是否有效。如果目錄無效或不存在，螢幕上將顯示對話方塊，告訴您選擇新的目錄。

接下來，配置程式會檢查 Application Server 實例連線是否處於作用中。如果不是，螢幕上將顯示對話方塊，警告您配置程式無法連線至指定的實例，您的配置無法完成。您可以接受指定的值或選擇新的 Application Server 配置值。

2. **Application Server 7.*x*：管理實例詳細資訊**

   輸入 Administration Server 連接埠號。例如：`4848`

   輸入 Administration Server 管理員的使用者 ID。例如：`admin`

   輸入管理員的使用者密碼。

   如果您要使用安全 Administration Server 實例，請核取 **[安全 Administration Server 實例]** 方塊。如果您不想使用該實例，則取消核取該方塊。

   按 **[下一步]** 以繼續，按 **[上一步]** 以返回前個一面板，或按一下 **[取消]** 以結束。

3. **預設網域分隔符號**

   僅當您要配置 Delegated Administrator 主控台時，此面板才會顯示。網域分隔符號是配置主控台所必需的；此資訊與 Web 容器無關。

   輸入使用者登入時要用於認證的預設網域分隔符號。例如：`@`。

4. **如果您要配置 Delegated Administrator 主控台：**

   - 如果您已選擇同時配置 Delegated Administrator 主控台和伺服器，請至

     第 63 頁的 「配置 Delegated Administrator 伺服器」
   - 如果您已選擇僅配置 Delegated Administrator 主控台 (連同所需的 Delegated Administrator 公用程式)，請至

     第 65 頁的 「完成配置」

   如果您要配置 Delegated Administrator 伺服器：

   請至

   第 63 頁的 「配置 Delegated Administrator 伺服器」中的步驟 3。

Application Server 8.*x* 配置

如果您要在 Application Server 8.*x* 上部署 Delegated Administrator 伺服器或主控台，請依照本小節中所述步驟執行。

▼ 配置 Application Server 8.*x*

步驟 **1. Application Server 8.*x* 配置詳細資訊**

面板文字會告訴您是否要爲 Delegated Administrator 伺服器或主控台提供 Application Server 8.*x* 配置資訊。

輸入 Application Server 安裝目錄。依預設，此目錄爲 `/opt/SUNWappserver/appserver`。

輸入 Application Server 網域目錄。依預設，此目錄爲 `/var/opt/SUNWappserver/domains/domain1`。

輸入 Application Server 文件根目錄。依預設，此目錄爲 `/var/opt/SUNWappserver/domains/domain1/docroot`。

您可以瀏覽以選取這些目錄中的任何目錄。

輸入 Application Server 目標名稱。例如：`server`。

輸入 Application Server 虛擬伺服器識別碼。例如：`server`。

輸入 Application Server 目標的 HTTP 連接埠號。

按 **[下一步]** 以繼續，按 **[上一步]** 以返回前一個面板，或按一下 **[取消]** 以結束。

配置程式會檢查您指定的目錄是否有效。如果目錄無效或不存在，螢幕上將顯示對話方塊，告訴您選擇新的目錄。

接下來，配置程式會檢查 Application Server 目標連線是否處於作用中。如果不是，螢幕上將顯示對話方塊，警告您配置程式無法連線至指定的目標，您的配置無法完成。您可以接受指定的值或選擇新的 Application Server 配置值。

2. Application Server 8.*x*：管理實例詳細資訊

輸入 Administration Server 連接埠號。例如：`4849`

輸入 Administration Server 管理員的使用者 ID。例如：`admin`

輸入管理員的使用者密碼。

如果您要使用安全 Administration Server 實例，請核取 **[安全 Administration Server 實例]** 方塊。如果您不想使用該實例，則取消核取該方塊。

按 **[下一步]** 以繼續，按 **[上一步]** 以返回前個一面板，或按一下 **[取消]** 以結束。

3. 預設網域分隔符號

僅當您要配置 Delegated Administrator 主控台時，此面板才會顯示。網域分隔符號是配置主控台所必需的；此資訊與 Web 容器無關。

輸入使用者登入時要用於認證的預設網域分隔符號。例如：`@`。

4. **如果您要配置 Delegated Administrator 主控台：**

   - 如果您已選擇同時配置 Delegated Administrator 主控台和伺服器，請至
     第 63 頁的 「配置 Delegated Administrator 伺服器」
   - 如果您已選擇僅配置 Delegated Administrator 主控台 (連同所需的 Delegated Administrator 公用程式)，請至
     第 65 頁的 「完成配置」

   如果您要配置 Delegated Administrator 伺服器：

   請至

   第 63 頁的 「配置 Delegated Administrator 伺服器」中的步驟 3。

配置 Delegated Administrator 伺服器

如果您已選擇配置 Delegated Administrator 伺服器，則配置程式將顯示以下面板。

▼ 配置 Delegated Administrator 伺服器

步驟

1. **Access Manager 基底目錄**
   輸入 Access Manager 基底目錄。預設目錄爲 `/opt/SUNWam`。

   按 **[下一步]** 以繼續，按 **[上一步]** 以返回前個一面板，或按一下 **[取消]** 以結束。

   配置程式會檢查是否已指定有效的 Access Manager 基底目錄。如果未指定，螢幕上將顯示對話方塊，指示必須選取現有的 Access Manager 基底目錄。

2. **接下來，螢幕上將顯示 Web 容器 [配置詳細資訊] 面板。**
   如果您已選擇配置主控台和伺服器，則這是第二次顯示 Web 容器 **[配置詳細資訊]** 面板。

   Delegated Administrator 伺服器會部署至與 Access Manager 相同的 Web 容器。(您無法爲 Delegated Administrator 伺服器選擇 Web 容器。)

   依照相應小節中的說明執行：

   - 第 59 頁的 「Web Server 配置」
   - 第 60 頁的 「Application Server 7.*x* 配置 」
   - 第 61 頁的 「Application Server 8.*x* 配置 」

3. **Directory (LDAP) Server**
   此面板要求有關連線至使用者/群組字尾的 LDAP 目錄伺服器的資訊。

   在文字方塊中輸入使用者和群組目錄伺服器 LDAP URL (**LdapURL**)、Directory Manager (**連結為**) 和密碼。

Directory Manager 在 Directory Server 和所有使用 Directory Server (例如 Delegated Administrator) 的 Sun Java System 伺服器上具有完全管理員權限，且具有對 Directory Server 中所有項目的完全管理存取權限。預設並建議的辨別名稱 (DN) 爲 `cn=Directory Manager`。

按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

4. **Access Manager 頂層管理員**

   輸入 Access Manager 頂層管理員的使用者 ID 和密碼。使用者 ID 和密碼在安裝 Access Manager 時建立。預設使用者 ID 爲 `amadmin`。

   按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

5. **Access Manager 內部 LDAP 認證密碼**

   輸入 Access Manager 內部 LDAP 認證使用者的密碼。

   認證使用者名稱程序內定爲 `amldapuser`。其由 Access Manager 安裝程式建立，是 LDAP 服務的連結 DN 使用者。

   按 [**下一步**] 以繼續，按 [**上一步**] 以返回前個一面板，或按一下 [**取消**] 以結束。

6. **組織辨別名稱 (DN)**

   輸入預設網域的組織 DN。例如，如果您的組織 DN 爲 `o=siroe.com`，則該組織中的所有使用者都將被置於 LDAP DN `o=siroe.com, o=usergroup` 下，其中 `o=usergroup` 爲您的根字尾。

   依預設，配置程式將預設網域增加至 LDAP 目錄中的根字尾下。

   如果您想在根字尾處 (而非在其下) 建立預設網域，請從顯示在 [**組織辨別名稱 (DN)**] 文字方塊中的 DN 中刪除組織名稱。

   例如，如果您的組織 DN 爲 `o=siroe.com`，根字尾爲 `o=usergroup`，則從文字方塊的 DN 中刪除 "`o=siroe.com`"，僅保留 `o=usergroup`。

   如果您選擇在根字尾處建立預設網域，而後來決定使用託管網域，則遷移至託管網域配置可能會很困難。`config-commda` 程式會顯示以下警告：

   「您選擇的組織 DN 是使用者/群組字尾。盡管該選擇有效，但是，如果您決定使用寄存網域，就會遇到移轉困難。如果您希望使用託管網域，請指定比使用者/群組字尾低一層級的 DN。」

   如需更多資訊，請參閱第 25 頁的 「支援一階式階層的目錄結構」。

   按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

7. **預設組織的頂層管理員**

   輸入要在預設網域 (組織) 中建立的頂層管理員的使用者 ID 和密碼。

   [**確認密碼**] 欄位會要求您再次輸入密碼。

   按 [**下一步**] 以繼續，按 [**上一步**] 以返回前一個面板，或按一下 [**取消**] 以結束。

8. **服務套裝軟體和組織範例**

   您可以選擇將服務套裝軟體範例和組織範例增加至 LDAP 目錄。

   載入服務套裝軟體範例。如果您要使用或修改服務套裝軟體範本範例以建立您自己的服務類別套裝軟體，請選取此選項。

   載入組織範例。如果您希望 LDAP 目錄樹狀結構包含提供者組織節點和從屬組織節點範例，請選取此選項。

   您可以選取

   - 服務套裝軟體範例和組織範例
   - 僅兩者之一
   - 二者皆不

   範例的喜好郵件主機。輸入安裝 Messaging Server 之機器的名稱。

   例如：`mymachine.siroe.com`

   如果您已選擇將組織範例載入 LDAP 目錄，則必須爲這些範例輸入喜好的郵件主機名稱。

   如需有關服務套裝軟體和組織的資訊，請參閱第 2 章：「Delegated Administrator 簡介」。

   執行配置程式後，您必須修改服務套裝軟體範本，以建立您自己的服務類別套裝軟體。如需有關此配置後作業的資訊，請參閱第 70 頁的 「建立服務套裝軟體」。

完成配置

執行本小節中所述的步驟，以完成執行配置程式。

▼ 完成配置

步驟

1. **準備配置**

   驗證面板會顯示將要配置的項目。

   按一下 [**立即配置**] 以開始配置，按 [**上一步**] 返回之前的面板以變更資訊，或按一下 [**取消**] 以結束。

2. **作業序列**

   正在執行之作業的序列顯示在 [作業序列] 面板上。這是實際配置發生的時間。

   面板顯示 [所有作業已通過] 時，您可以按 [**下一步**] 以繼續，或按一下 [**取消**] 以阻止執行作業並結束。

   螢幕上將顯示對話方塊，提醒您重新啓動 Web 容器以使配置變更生效。

3. **安裝摘要**

   [安裝摘要] 面板將顯示已安裝的產品以及可顯示有關此配置的更多資訊的 **[詳細資訊...]** 按鈕。

   `config-commda` 程式的記錄檔在 `/opt/SUNWcomm/install` 目錄中建立。該記錄檔的名稱爲 `commda-config_`*`YYYYMMDDHHMMSS`*`.log`，其中 *YYYYMMDDHHMMSS* 表示配置的 4 位數年份、月份、日期、小時、分鐘和秒。

   按一下 **[關閉]** 以完成配置。

重新啓動 Web 容器

完成 Delegated Administrator 配置後，您必須重新啓動 Delegated Administrator 部署至的 Web 容器 (以下之一)：

- Web Server
- Application Server 7.x
- Application Server 8.x

`config-commda` 程式建立的配置檔案和記錄檔

配置檔案

`config-commda` 程式使用您在面板中提供的資訊爲三個 Delegated Administrator 元件建立以下配置檔案：

- Delegated Administrator 公用程式：

  配置檔案名稱：`cli-usrprefs.properties`

  預設位置：`/var/opt/SUNWcomm/config`

- Delegated Administrator 伺服器：

  配置檔案名稱：`resource.properties`

  預設位置：

  `/opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet`

  或者

  `/var/opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet`

- Delegated Administrator 主控台：

  配置檔案名稱：`daconfig.properties`

  預設位置：

  `/opt/SUNWcomm/WEB-INF/classes/com/sun/comm/da/resources`

或者

`/var/opt/SUNWcomm/WEB-INF/classes/com/sun/comm/da/resources`

如需有關這些檔案、它們包含的特性以及如何編輯這些特性以自訂配置的資訊，請參閱第 4 章。

記錄檔

Delegated Administrator 主控台可建立執行階段記錄檔：

預設記錄檔名稱：`da.log`

預設位置：`/opt/SUNWcomm/log`

如需有關此記錄檔和其他 Delegated Administrator 記錄檔的更多資訊，請參閱附錄 C。

執行無訊息安裝

Delegated Administrator 公用程式初始執行階段配置程式會自動建立無訊息安裝狀態檔案 (稱爲 `saveState`)。此檔案包含有關配置程式的內部資訊，用於執行無訊息安裝。

無訊息安裝 `saveState` 檔案儲存在 `/opt/SUNWcomm/data/setup/commda-config_`*YYYYMMDDHHMMSS*`/` 目錄中，其中 *YYYYMMDDHHMMSS* 表示 `saveState` 檔案的 4 位數年份、月份、日期、小時、分鐘和秒。

例如，一旦已執行一次 `config-commda` 程式，您便可以在無訊息安裝模式中執行該程式：

```
da_base/sbin/config-commda -nodisplay -noconsole -state
 fullpath/saveState
```

fullpath 變數是 `saveState` 檔案所在目錄的完整目錄路徑。

執行 Delegated Administrator 主控台和公用程式

啓動主控台

透過存取 Delegated Administrator 主控台部署至的 Web 容器來啓動 Delegated Administrator 主控台。

▼ 啓動 Delegated Administrator 主控台

步驟 **1. 請至以下 url：**

`http://` *host*`:`*port*`/da/DA/Login`

其中

host 是 Web 容器主機電腦

port 是 Web 容器連接埠

例如：

`http://siroe.com:8080/da/DA/Login`

螢幕上將顯示 Delegated Administrator 主控台登入視窗。

2. 登入 Delegated Administrator 主控台。

您可以使用在 Delegated Administrator 配置程式中指定的頂層管理員 (TLA) 的使用者 ID 和密碼。在以下面板中需要此資訊：

預設組織的頂層管理員

備註 – 執行 Delegated Administrator 主控台時，在 Access Manager 中設定的值可以決定階段作業逾時。如需有關階段作業逾時值的資訊，請參閱「*Sun Java System Access Manager Administration Guide*」中的「Session Service Attributes」。如需有關在 Access Manager 主控台中檢視這些值的資訊，請參閱「*Sun Java System Access Manager Administration Guide*」中的「Current Sessions」。

執行指令行公用程式

您可以透過輸入指令名稱 commadmin，從終端機視窗執行 Delegated Administrator 公用程式。

▼ 執行指令行公用程式

步驟

1. **請至 *da_base*/bin/ 目錄。例如，至 /opt/SUNWcomm/bin/。**
2. **輸入 commadmin 指令。**

範例 3–1 使用 commadmin 搜尋使用者

以下指令可在 varrius.com 網域中搜尋使用者：

```
commadmin user search -D chris -w bolton -d varrius.com -n sesta.com
```

如需有關此 commadmin 指令的詳細資訊，請參閱第 127 頁的 「commadmin user search」。

更多資訊 commadmin 回覆碼

提示 – commadmin 作業成功時，指令行上會顯示 OK 訊息。

如果失敗，會顯示以下訊息：

```
FAIL
<message>
```

其中 <*message*> 顯示錯誤文字。

配置後作業

執行 Delegated Administrator 配置程式後，您應執行以下作業：

- 第 70 頁的 「將郵件服務和行事曆服務增加至預設網域」
- 第 70 頁的 「建立服務套裝軟體」

僅當您在 Schema 2 相容模式中使用 LDAP 目錄時，才執行以下作業：

- 第 75 頁的 「爲 Schema 2 相容模式增加 ACI」

將郵件服務和行事曆服務增加至預設網域

config-commda 程式會建立預設網域。

如果您要在預設網域中建立具有郵件服務或行事曆服務的使用者，則首先必須將郵件服務和行事曆服務增加至該網域中。

若要執行此作業，請使用帶有 -S mail 和 -S cal 選項的 commadmin domain modify 指令。

以下範例顯示如何使用 commadmin domain modify 將郵件服務和行事曆服務增加至預設網域：

```
commadmin domain modify -D chris -w bolton -n sesta.com -d siroe.com
 -S mail,cal -H test.siroe.com
```

如需 commadmin 指令語法及詳細資訊，請參閱第 5 章。

建立服務套裝軟體

使用 Delegated Administrator 在 LDAP 目錄中佈建的每個使用者和群組都應具有服務套裝軟體。使用者或群組可以具有多個服務套裝軟體。

預先定義的服務類別範本

執行 Delegated Administrator 配置程式 (config-commda) 時，您可以選擇使用 config-commda 程式在目錄中安裝服務類別範本範例。

如需有關服務套裝軟體中可用的服務類別範本範例和郵件屬性的資訊，請參閱第 1 章中的第 30 頁的 「服務套裝軟體」。

您可以使用服務類別範本範例建立和指定服務套裝軟體。但是，範本範例僅做爲範例。

建立您自己的服務套裝軟體

很多時候，您可能希望使用適用於您的安裝中的使用者和群組之屬性值，根據自訂的服務類別範本建立自己的服務套裝軟體。

若要建立您自己的服務套裝軟體，請使用儲存在 da.cos.skeleton.ldif 檔案中的服務類別範本。

特別建立此檔案以用做撰寫自訂服務類別範本的範本。配置 Delegated Administrator 時，此檔案未安裝在 LDAP 目錄中。

da.cos.skeleton.ldif 包含四個參數化範本，Delegated Administrator 提供的每個服務類別定義均對應一個範本：

- standardUserMail
- standardUserCalendar
- standardUserMailCalendar
- standardGroupMail

您可以使用 da.cos.skeleton.ldif 檔案中的一個或多個參數化範本建立自己的服務類別範本。

da.cos.skeleton.ldif 檔案中的服務類別範本如下：

```
# Templates for creating COS templates for service packages.
#
# There are four COS definitions :
#   standardUserMail
#   standardUserCalendar
#   standardUserMailCalendar
#   standardGroupMail
#
# Each definition can have zero or more COS templates which
# define specific values for the attributes listed in the
# COS definition.
#
# Each COS definition points to a corresponding subdirectory
# in which COS templates for that definition (and no other
# definition) are found.  The templates directory structure
# is as follows:
# standardUserMail          => o=mailuser,o=costemplates,<ugldapbasedn>
# standardUserCalendar      => o=calendaruser,o=costemplates,
#                                <ugldapbasedn>
# standardUserMailCalendar  => o=mailcalendaruser,o=costemplates,
#                                <ugldapbasedn>
# standardGroupMail          => o=mailgroup,o=costemplates,
#                                <ugldapbasedn>
#
# Thus, all COS templates for the user mail service are found in the
# o=mailuser,o=costemplates,<ugldapbasedn> directory, etc.
#
# It is not necessary to have any templates for a given definition.
# In that case default values are assumed for those attributes defined
# in the COS definition.
#
# If a template is created for a definition there should be at least
# one attribute with a defined value.
#
# Consult documentation for values for the attributes.
# Documentation includes units and default values.
#
# The finished COS derived from this skeleton is added to the
# directory with the following command:
#
# ldapmodify -D <directory manager> -w <password>
# -f <cos.finished.template.ldif>
#
#
################################################################
```

```
#
#    standardMailUser COS template
#
###############################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
# - mailMsgQuota
# - mailAllowedServiceAccess
#
dn: cn=<service package name>,o=mailuser,o=cosTemplates,<rootSuffix>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
mailQuota: <ma:ilQuotaValue>
mailMsgQuota: <mailMsgQuotaValue>
mailAllowedServiceAccess: <mailAllowedServiceAccessValue>
#
#
###############################################################
#
#    standardCalendarUser COS template
#
###############################################################
# There must be a least one of the following attributes:
# - icsPreferredHost
# - icsDWPHost
# - icsFirstDay
#
dn: cn=<service package name>,o=calendaruser,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
icsPreferredHost: <preferredHostValue>
icsDWPHost: <dwpHostValue>
icsFirstDay: <firstDayValue>
daServiceType: calendar user
#
#
###############################################################
#
#    standardMailCalendarUser COS template
#
###############################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
```

```
# - mailMsgQuota
# - mailAllowedServiceAccess
#
dn: cn=<service package name>,o=mailcalendaruser,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
mailquota: <mailQuotaValue>
mailmsgquota: <mailMsgQuotaValue>
mailAllowedServiceAccess: <mailAllowedServiceAccessValue>
daServiceType: calendar user
daServiceType: mail user
#
#
################################################################
#
#    standardMailGroup COS template
#
################################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
#
#
dn: cn=<service package name>,o=mailgroup,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
daServiceType: mail group
```

▼ 建立您自己的服務套裝軟體

步驟 **1. 複製並重新命名 `da.cos.skeleton.ldif` 檔案中的一個參數化範本。**

安裝 Delegated Administrator 時，`da.cos.skeleton.ldif` 檔案安裝在以下目錄中：

da_base`/lib/config-templates`

選擇 `da.cos.skeleton.ldif` 檔案中以下範本中的其中一個範本，以複製並重新命名：

```
standardUserMail
standardUserCalendar
```

```
standardUserMailCalendar
standardGroupMail
```

2. **在範本副本中編輯以下參數：**

   - `<ugldapbasedn>`

     將根字尾參數 `<rootSuffix>` 變更爲您的根字尾 (如 `o=usergroup`)。

     `<ugldapbasedn>` 參數將顯示在 DN 中。

   - `<service package name>`

     將 `<service package name>` 參數變更爲您自己的服務套裝軟體名稱。

     `<service package name>` 參數將顯示在 DN 和 `cn` 中。

   - 郵件屬性值：

     ```
     <mailMsgMaxBlocksValue>
     <mailQuotaValue>
     <mailMsgQuotaValue>
     <mailAllowedServiceAccessValue>
     ```

     按照規格編輯這些值。

     例如，您可以爲郵件屬性輸入以下值：

     ```
     mailMsgMaxBlocks: 400
     mailQuota: 400000000
     mailMsgQuota: 5000
     mailAllowedServiceAccess: imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
     ```

   - 行事曆屬性值：

     ```
     <preferredHostValue>
     <dwpHostValue>
     <firstDayValue>
     ```

     這些參數代表 `icsPreferredHost`、`icsDWPHost` 和 `icsFirstDay` LDAP 屬性的值。

     按照規格編輯這些值。

   如需這些屬性的定義和說明，請參閱「*Sun Java System Communications Services Schema Reference*」中的「Chapter 3:Messaging Server and Calendar Server Attributes」。

   您必須在自訂的服務類別範本中至少使用一個屬性。您不必在自訂範本中使用全部四個郵件屬性。您可以刪除服務套裝軟體中的一個或多個屬性。

3. **使用 LDAP 目錄工具 `ldapmodify` 在目錄中安裝服務套裝軟體。**

   例如，您可以執行以下指令：

   ```
   ldapmodify -D <directory manager> -w <password> -f
   <cos.finished.template.ldif>
   ```

   其中

<directory manager> 是 Directory Server 管理員的名稱。

<password> 是 Directory Service 管理員的密碼。

<cos.finished.template.ldif> 是要在目錄中做爲服務套裝軟體安裝的已編輯 ldif 檔案的名稱。

爲 Schema 2 相容模式增加 ACI

如果您要在 Schema 2 相容模式中使用 LDAP 目錄，則必須手動將 ACI 增加至目錄，以使 Delegated Administrator 可以在目錄中佈建。執行以下步驟：

▼ 爲 Schema 2 相容模式增加 ACI

步驟 **1. 將以下兩個 ACI 增加至 OSI 根。您可以在位於 `/opt/SUNWcomm/config` 目錄中的 `usergroup.ldif` 檔案中找到以下兩個 ACI。**

確定使用 usergroup 字尾替代 ugldapbasedn。將已編輯的 usergroup.ldif 增加至 LDAP 目錄。

```
#
# acis to limit Org Admin Role
#
########################################
# dn: <local.ugldapbasedn>
########################################
dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)

dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read
to org node";
allow (read,search) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)
```

2. 將以下兩個 ACI 增加至 DC 樹狀結構根字尾。您可以在位於 `/opt/SUNWcomm/config` 目錄中的 `dctree.ldif` 檔案中找到以下兩個 ACI。

確定使用 DC 樹狀結構根字尾替代 *dctreebasedn*，使用 usergroup 字尾替代 *ugldapbasedn*。將已編輯的 dctree.ldif 增加至 LDAP 目錄。

```
#
# acis to limit Org Admin Role
#
```

```
########################################
# dn: <dctreebasedn>
########################################
dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to dc node";
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)

dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to dc
node"; allow (read,search) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)
```

3. **將以下附加 ACI 增加至 DC 樹狀結構根字尾。(這些 ACI 不在 `dctree.ldif` 檔案中。)**

```
dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Proxy user rights"; allow (proxy)
userdn = "ldap:///cn=puser,ou=DSAME Users,<ugldapbasedn>";)

dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the
root suffix"; allow (all) userdn ="ldap:///cn=dsameuser,ou=DSAME
Users,<ugldapbasedn>";)

dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Top-level admin rights";
allow (all) roledn = "ldap:///cn=Top-level Admin
Role,<ugldapbasedn>";)
```

4. **將 `AMConfig.properties` 檔案中的 `com.iplanet.am.domaincomponent` 特性設定為您的 DC 樹狀結構根字尾。**

   例如，修改 <*AM_base_directory*>`/lib/AMConfig.properties` 檔案中的以下各行：

   從

   ```
   com.iplanet.am.domaincomponent=o=isp
   ```

   至

```
com.iplanet.am.domaincomponent=o=internet
```

5. **允許 Access Manager (以前稱為 Identity Server) 使用相容模式。**
   在 Access Manager 主控台中，在 [Administration Console 服務] 頁面中核取 (啓用) **[已啓用網域元件樹狀結構]** 核取方塊。

6. **將 `inetdomain` 物件類別增加至所有 DC 樹狀結構節點 (如 `dc=com,o=internet`)，如以下範例所示：**

```
/var/mps/serverroot/shared/bin 298% ./ldapmodify
-D "cn=Directory Manager" -w password
dn: dc=com,o=internet
changetype: modify
add: objectclass
objectclass: inetdomain
```

7. **重新啓動 Web 容器。**

第 4 章

自訂 Delegated Administrator

使用配置程式 (`config-commda`) 安裝和配置 Delegated Administrator 之後，您可以自訂配置以滿足特定需要。本章提供了如何自訂特定 Delegated Administrator 功能的範例。

您應該先備份現有的 Delegated Administrator 配置檔案，然後再開始對其進行自訂。

而且，在升級 Delegated Administrator 時，會遺失自訂的配置資料。因此，您應該在升級 Delegated Administrator 之前保留自訂配置，或重新執行 Delegated Administrator 配置程式。 如需更多資訊，請參閱第 52 頁的 「保留現有配置」。

本章說明以下主題：

使用服務範圍預設配置喜好的郵件主機

如果您想使用伺服器範圍預設來設定喜好的郵件主機和喜好的郵件儲存，則可以執行本小節中所述的作業。

如果您需要從主控台 (特別是從 [新建組織精靈] 和 [組織特性] 螢幕) 移除 [喜好的郵件主機] 欄位，則應執行以下步驟：

- 編輯 `Security.properties` 檔案。本小節中說明了此步驟。
- 啓用 MailHostStorePlugin。下一小節第 81 頁的 「爲 Delegated Administrator 增加外掛程式」中說明了此步驟。

Security.properties 檔案可讓您爲所有角色或個別角色自訂 Delegated Administrator 主控台。

Security.properties 檔案位於目錄 *da_base*/da/WEB-INF/classes/com/sun/comm/da/resources 中

若要從主控台移除 [喜好的郵件主機]，請將下面顯示的各行增加至 Security.properties 檔案：

```
# Remove Preferred Mail Host from UI
*.NewOrganizationPage6.PreferredMailHostProperty=INVISIBLE
*.NewOrganizationSummaryPage.PreferredMailHostSummaryProperty=INVISIBLE
*.OrgProperties.MailHostName=INVISIBLE
*.OrgProperties.MailHostNameText=INVISIBLE
*.OrgProperties.MailHostValue=INVISIBLE
```

注意：您可以將這些行增加至此檔案以進行自訂，但請勿編輯已存在的行。編輯現有行會導致主控台上丟出異常。

檔案中特性的格式爲：*Security Element Name=Permission*

安全元素名稱的格式爲：*Role Name* .*Container View Name*. *Console Element Name*

安全元素可指定主控台元素及爲其定義權限的角色。如果您不知道元素名稱，請檢視頁面來源以將該頁面上的名稱與您感興趣的主控台元素進行對比。

該頁面上的名稱是完全合格的名稱。您只需挑選名稱的最後兩個元素，這兩個元素形成 *Container View Name* .*Console Element Name*。

Delegated Administrator 的有效角色名稱如下：

「ProviderAdminRole」(SPA)，如需有關此角色的資訊，請參閱附錄 A。

「OrganizationAdminRole」(OA)

「Top-levelAdminRole」(TLA)

「*」(除非已將權限強加給特定角色，否則將其套用至所有角色)

權限必須是以下字串之一：

- EDITABLE – 指示安全元素可編輯。
- NONEDITABLE – 指示安全元素唯讀。
- VISIBLE – 指示安全元素可見且唯讀。
- INVISIBLE – 指示安全元素不可見。

爲 Delegated Administrator 增加外掛程式

您可以自訂 Delegated Administrator 以支援以下外掛程式：

- `MailHostStorePlugin`

  依預設，停用此外掛程式。如果在建立商務組織時未提供 `preferredmailhost`，則將產生異常。如果啓用該外掛程式，則僅當缺少相應屬性時才使用平面檔案 (本小節中稍後說明) 中的值。

- `MailDomainReportAddressPlugin`

  使用網域值可傳回所需的 DSN 位址。預設實作是傳回字串 `MAILER-DAEMON@<`*domain* `>`。

- `UidPlugin`

  產生唯一的 ID 字串。預設實作產生 GUID 以傳回給呼叫者。

啓用外掛程式

若要啓用這些外掛程式，請編輯 `commcli servlet resource.properties` 檔案，該檔案位於以下目錄中：

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

(依預設，*da_base* 爲 `/opt/SUNWcomm`。)

外掛程式位於開頭如下的區段中的 `resource.properties` 檔案中：

```
#########################
# Plugin Configuration #
#########################
```

每個都以「`plugin`」做爲字尾。目前的清單如下：

```
jdapi-mailhoststoreplugin=disabled

jdapi-mailhoststorepluginclass=sun.comm.cli.server.util.MailHostStorePlugin
jdapi-mailhoststorepluginfile=/tmp/mailhostmailstore
jdapi-maildomainreportaddressplugin=enabled
jdapi-maildomainreportaddresspluginclass=sun.comm.cli.server.
  util.MailDomainReportAddressPlugin
jdapi-uidautogenerationplugin=disabled
jdapi-uidautogenerationpluginclass=sun.comm.cli.server.util.UidPlugin
```

外掛程式格式

每個外掛程式都至少具有兩行，其格式如下：

- jdapi-<*name*>plugin= "enabled" | "disabled"
-

  jdapi-<*name*>pluginclass=sun.comm.cli.server.util/
  <*java class name*>

若要啓用外掛程式，請將「disabled」變更爲「enabled」。

提供了本小節中列出的所有外掛程式的外掛程式類別。這些類別位於以下目錄中：

da_base/data/WEB-INF/classes/sun/comm/cli/server/util

您無需對這些類別執行任何作業。

MailHostStorePlugin 所需的附加平面檔案

MailHostStorePlugin 需要包含在外掛程式第三行中的平面檔案。外掛程式讀取平面檔案中的值並用其設定屬性值。如果啓用外掛程式，則該檔案必須存在，否則將發生錯誤。

-

```
jdapi-mailhoststoreplugin
    o jdapi-mailhoststorepluginin=<full file name>
    o file has one line
    o value is that for :
        o preferredmailhost attribute
        o preferredmailmessagestore attribute
    o form
        o <mailhost>:<mailpartition>
```

建立 LDAP 物件時增加自訂物件類別

您可以啓用 Delegated Administrator 以將自訂物件類別增加至新使用者、群組、資源或組織的 LDAP 項目中。若要完成此作業，您可以透過 Access Manager 自訂安裝在目錄中的相應的物件建立範本。

例如，BasicUser 建立範本可決定建立新使用者時增加至使用者項目的物件類別和屬性。您可以使用自訂物件類別更新 BasicUser 建立範本。之後，自訂物件類別將與標準物件類別一起增加至每個新的使用者項目中。

以下程序說明如何自訂 BasicUser 範本。您可以依照相同的程序自訂 BasicGroup、BasicResource 和 BasicOrganization 建立範本。

▼ 將自訂物件類別增加至使用者建立程序

步驟 **1. 確定在目錄模式中定義自訂物件類別。**

2. 找到以下目錄項目：

```
ou=basicuser,ou=creationtemplates,ou=templates,ou=default,
ou=globalconfig,ou=1.0,ou=dai,ou=services,
o=$Root_Suffix
```

其中 *$Root_Suffix* 是目錄的根字尾。

3. 將以下 *attribute:value* 增加至項目：

```
sunkeyValue:required=objectClass=$Your_Custom_Objectclass.
```

其中 *$Your_Custom_Objectclass* 是自訂物件類別。

自訂使用者登入

執行 Delegated Administrator 配置程式 (`config-commda`) 時，用於登入 Delegated Administrator 的值設定爲 `uid`。

例如，如果您想要以 TLA 的身份登入，且 TLA 的 `uid` 爲 `john.doe`，則應使用 `john.doe` 登入 Delegated Administrator。

您可以自訂 Delegated Administrator，以便可以使用使用者登入的附加值。例如，您可以增加郵件位址 (`mail`)。

如何設定使用者登入值

`config-commda` 程式可使用 `resource.properties` 檔案中的 loginAuth-idAttr 特性將此值設定爲 `uid`，如以下範例所示：

```
loginAuth-searchBase=<$rootSuffix>
         servicepackage-cosdefbasedn = <$rootSuffix>
          loginAuth-idAttr-1=uid
```

其中 *<$rootSuffix>* 是目錄的根字尾。

`resource.properties` 檔案位於

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties` 中

增加使用者登入值

您可以透過編輯 resource.properties 檔案來設定使用者登入的附加值。

例如，爲了可以使用郵件位址 (如 john.doe@sesta.com) 登入，您應將以下行增加至 resource.properties 檔案：

```
loginAuth-searchBase=<$rootSuffix>
         servicepackage-cosdefbasedn = <$rootSuffix>
          loginAuth-idAttr-1=uid
          loginAuth-idAttr-2=mail
```

其中 *<$rootSuffix>* 是目錄的根字尾。

請注意，您必須將增量增加至每個新值的 loginAuth-idAttr 特性。在此範例中，已增加第二個值，因此應將 -2 增加至 loginAuth-idAttr。

您可以增加 loginAuth-idAttr 特性的多個實例：

```
loginAuth-idAttr-1=uid
  loginAuth-idAttr-2=mail
  |
  loginAuth-idAttr-n=<login-in value>
```

新使用者需要服務套裝軟體

依預設，Delegated Administrator 可讓您建立新使用者，但不會爲該使用者指定服務套裝軟體。

您可以變更預設，讓所有新使用者都必須至少具有一個服務套裝軟體。

▼ 要求新的使用者具有服務套裝軟體

步驟

1. **在文字編輯器中開啓 daconfig.properties 檔案。**
   依預設，daconfig.properties 檔案位於以下目錄中：

   ```
   /var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/
   comm/da/resources/daconfig.properties
   ```

2. **將 user.atleastOneServicePackage 特性的值從 false 變更為 true。**
   依預設，此值爲 false。

   例如：

   ```
   user.atleastOneServicePackage=true
   ```

將此值設定爲 true 後，當您使用 Delegated Administrator 主控台中的 [建立新使用者] 精靈時，必須至少指定一個服務套裝軟體以成功建立新使用者。

增加新的行事曆時區

您可以透過增加新的 Calendar Server 時區來自訂 Delegated Administrator。Delegated Administrator 便可使用新時區佈建組織、使用者、群組和資源。

增加時區後，您可以將其設定爲新建立使用者的預設時區。

▼ 在 Delegated Administrator 中增加新時區

步驟

1. **在 Calendar Server 中增加時區。**

   若要完成此步驟，您必須編輯 timezones.ics 檔案及其他 Calendar Server 檔案。如需說明，請參閱「Sun Java System Calendar Server Administration Guide」中「Managing Calendar Server Time Zones」一章中的「Adding a New Time Zone」。

2. **備份 `UserCalendarService.xml`、`DomainCalendarService.xml` 和 `Resources.properties` 檔案。**

   依預設，xml 檔案位於以下目錄中：

   ```
   /opt/SUNWcomm/lib/services
   ```

   依預設，Resources.properties 檔案位於以下目錄中：

   ```
   /var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/ \
   comm/da/resources
   ```

   另外，確定在升級 Delegated Administrator 之前保留自訂配置資料，或重新執行 Delegated Administrator 配置程式。

3. **編輯 `UserCalendarService.xml` 和 `DomainCalendarService.xml` 檔案，以在 Delegated Administrator 中增加新時區。**

   依預設，這些 xml 檔案位於以下目錄中：

   ```
   /opt/SUNWcomm/lib/services
   ```

   - 在 UserCalendarService.xml 和 DomainCalendarService.xml 檔案中找到以下項目標題：

     ```
     <AttributeSchema name="icstimezone"
                                type="single choice"
                                syntax="string"
     ```

```
                                    any="optional|adminDisplay">
                                    <ChoiceValues>
```

- 將新的時區值增加至 <ChoiceValues> 清單中。

4. **執行 Access Manager amadmin 公用程式，以刪除目前的服務並增加已更新的服務。**

   對於 UserCalendarService.xml 和 DomainCalendarService.xml 檔案，執行以下 amadmin 指令：

```
./amadmin -u <admin> -w <password> -r DomainCalendarService
```

```
./amadmin -u <admin> -w <password> -s $PATH/DomainCalendarService.xml
```

備註 – 如果您還想將新時區設定爲預設時區，則可以在執行這兩項作業後執行這些 amadmin 指令。(以下作業說明如何變更預設時區。)

---

5. **重新啓動 Web 容器，以使變更生效。**

▼ 變更 Delegated Administrator 中的預設時區

步驟

1. **在 UserCalendarService.xml 和 DomainCalendarService.xml 檔案中編輯以下值：**

```
<DefaultValues>
                <Value>America/Denver</Value>
</DefaultValues>
```

   您可以在 xml 檔案的以下項目下找到 <DefaultValues>：

```
<AttributeSchema name="icstimezone"
```

2. **執行 Access Manager amadmin 公用程式，以刪除目前的服務並增加已更新的服務。**

   對於 UserCalendarService.xml 和 DomainCalendarService.xml 檔案，執行以下 amadmin 指令：

```
./amadmin -u <admin> -w <password> -r DomainCalendarService
```

```
./amadmin -u <admin> -w <password> -s $PATH/DomainCalendarService.xml
```

3. **重新啓動 Web 容器，以使變更生效。**

▼ 將新時區增加至 Delegated Administrator 主控台

步驟

- **編輯 `Resources.properties` 檔案，該檔案位於 Delegated Administrator 資料目錄下。**

  依預設，`Resources.properties` 檔案位於以下目錄中：

  ```
  /var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/ \
  comm/da/resources
  ```

  若要編輯 `Resources.properties`，請搜尋 `rsrc.Timezone` 特性，並將新時區增加至相應的清單中。

  編輯此檔案之後，新時區將顯示在 Delegated Administrator 主控台中的相應清單方塊中。

第 5 章

指令行公用程式

Delegated Administrator 指令行公用程式可讓管理員管理不同的使用者、群組、網域及組織通訊服務。本章說明用於執行大批量作業，如建立、修改、刪除及搜尋使用者、群組、網域及組織的指令行工具集。

指令

這些指令在下表中列出。該表格由三欄組成；第一欄列出指令，第二欄爲指令說明，第三欄爲允許執行該指令的管理員類型。

`commadmin` 公用程式位於 `/opt/SUNWcomm/bin` 目錄中。

表 5–1 Delegated Administrator 指令行介面

指令	說明	可以執行該指令的人員*
第 93 頁的 「commadmin admin add」	授予使用者組織管理員權限	頂層管理員
第 94 頁的 「commadmin admin remove」	撤銷使用者的組織管理員權限	頂層管理員
第 95 頁的 「commadmin admin search」	搜尋並顯示擁有組織管理員權限的使用者	頂層管理員、組織管理員
第 96 頁的 「commadmin domain create」	建立網域	頂層管理員
第 99 頁的 「commadmin domain delete」	刪除網域	頂層管理員

表 5–1 Delegated Administrator 指令行介面　(續)

指令	說明	可以執行該指令的人員*
第 100 頁的 「commadmin domain modify」	修改網域	頂層管理員
第 102 頁的 「commadmin domain purge」	清除網域	頂層管理員
第 104 頁的 「commadmin domain search」	搜尋網域	頂層管理員
第 105 頁的 「commadmin group create」	建立群組	頂層管理員、組織管理員和郵件清單所有者
第 107 頁的 「commadmin group delete」	刪除群組	頂層管理員、組織管理員和郵件清單所有者
第 109 頁的 「commadmin group modify」	修改群組	頂層管理員、組織管理員和郵件清單所有者
第 111 頁的 「commadmin group search」	搜尋群組	任何人
第 113 頁的 「commadmin resource create」	建立資源	頂層管理員、組織管理員
第 117 頁的 「commadmin resource modify」	修改資源	頂層管理員、組織管理員
第 115 頁的 「commadmin resource delete」	刪除資源	頂層管理員、組織管理員
第 118 頁的 「commadmin resource search」	搜尋資源	任何人
第 120 頁的 「commadmin user create」	建立使用者	頂層管理員、組織管理員
第 122 頁的 「commadmin user delete」	刪除使用者	頂層管理員、組織管理員
第 127 頁的 「commadmin user search」	搜尋使用者	任何人
第 124 頁的 「commadmin user modify」	修改使用者	頂層管理員、組織管理員
*此發行版本的 Delegated Administrator 不支援服務提供者管理員使用 `commadmin` 公用程式。		

執行模式

可在三種模式中執行指令行：

- 使用檔案中指定的選項執行

  `commadmin` *object task* `-i` *inputfile*

  分析並執行 *inputfile*。
- *互動*

  `commadmin` *object task*

  會詢問管理員選項和屬性的剩餘部分。
- 立即執行或 Shell 執行

  `commadmin` *object task* [*options*]

`commadmin` 作業成功時，指令行上會顯示 OK 訊息。

如果失敗，會顯示以下訊息：

`FAIL`

<message>

其中，*<message>* 顯示錯誤文字。

指令檔格式

使用 `-i` 選項可以在檔案中指定這些選項。

在檔案中，選項名稱和選項值以空格分隔。選項值以第一個非空格字元開始，並延伸至行尾字元。選項集以空行分隔。

一般語法爲：

```
<option name><white space>[option value, if any]
<option name><white space>[option value, if any]
...
<option name><white space>[option value, if any]
<blank line>
<option name><white space>[option value, if any]
<option name><white space>[option value, if any]
...
<option name><white space>[option value, if any]
```

指令行中給定的選項值成爲每個選項集的預設值。或者，可以爲每個選項集指定這些選項。然後該值將置換所有在指令行上指定的預設值。

以下是由 `commadmin user add` 指令的 `-i` 選項指定的檔案之格式和語法範例。

```
l newuser1
F new
L user1
W secret

l newuser2
F new
L user2
W secret

l newuser3
F new
L user3
W secret

<and so forth...>
```

指令說明

本小節提供指令行工具的說明、語法及範例。

必要的 commadmin 選項

以下是用於認證管理員或使用者的必要的選項。

選項	說明
`-D` *userid*	用於連結至目錄的使用者 ID。
`-w` *password*	用於認證目錄的使用者 ID 的密碼。 也可以透過文字檔 *password*`.txt` 指定 *password*。
`-n` *domain*	管理員所屬的網域。

Access Manager 主機 (`-X`)、Access Manager 連接埠 (`-p`) 及預設網域 (`-n`) 值在安裝期間指定，並儲存於 `cli-userprefs.properties` 檔案中。

備註 – 如果 -X、-p 及 -n 選項未在執行 commadmin 指令時指定，則將從 cli-userprefs.properties 檔案中取得這些選項的值。

commadmin admin add

commadmin admin add 指令將授予特定網域的使用者組織管理員權限。只有頂層管理員或 ISP 管理員可以執行此指令。

語法

commadmin admin add -D *login* -l *login* -n *domain* -w *password* -d *domain* [-h] [-i *inputfile*] [-p *AM port*] [-X *AM host*] [-?] [-s] [-v] [-V]

選項

以下選項是必要的：

選項	說明
-D *login*	頂層管理員的使用者 ID。
-l *login*	要授予組織管理權限的使用者之使用者 ID。使用者應該存在於目錄中，且是由 -d 選項指定之網域的一部分。
-n *domain*	頂層管理員所在的網域。如果未指定，則使用 cli-userprefs.properties 檔案中儲存的預設網域。
-w *password*	頂層管理員的密碼。
-d *domain*	要授予其管理權限的網域。如果未指定，則使用由 -n 選項指定的網域。

以下選項是非必要的：

選項	說明
-i *inputfile*	參閱檔案而非指令行中的指令資訊。
-p *AM port*	使用此選項指定 Access Manager 偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。

選項	說明
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*
`-h`、`-?`	顯示指令用法語法。
`-V`	顯示有關公用程式及其版本的資訊。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-v`	啓用除錯輸出。

範例

以下指令授予使用者 ID 爲 `admin1` 的使用者組織管理員權限。

```
commadmin admin add -D chris -n sesta.com -w bolton -l admin1 \
-d florizel.com
```

以下指令授予網域 `florizel.com` 中使用者 ID 爲 `admin2` 的使用者組織管理員權限。

```
commadmin add admin -D chris -w bolton -l admin2 -n varrius.com \
-d florizel.com
```

commadmin admin remove

`commadmin admin remove` 指令可移除現有組織管理員的組織管理員權限。只有頂層管理員可以執行此指令。

若要移除多個使用者的組織管理員權限，請使用 `-i` 選項。

語法

`commadmin admin remove -D` *login* `-l` *login* `-n` *domain* `-w` *password* `-d` *domain name* `[-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-X` *AM host*`] [-s] [-v] [-V]`

選項

以下選項是必要的：

選項	說明
`-D` *login*	頂層管理員的使用者 ID。
`-l` *login*	需要撤銷其管理員權限的使用者之使用者 ID。

選項	說明
-n *domain*	頂層管理員所在的網域。
-w *password*	頂層管理員的密碼。
-d *domain name*	要撤銷其管理員權限的網域。如果未指定 -d，則使用由 -n 指定的網域。

以下選項是非必要的：

選項	說明
-h、-?	顯示指令用法語法。
-i *inputfile*	參閱檔案而非指令行中的指令資訊。
-p *AM port*	使用此選項指定 Access Manager 偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
-x *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。
-s	使用 SSL (安全通訊端層) 連線 Access Manager。
-v	啓用除錯輸出。
-V	顯示有關公用程式及其版本的資訊。

範例

以下指令可撤銷使用者 ID 爲 admin5 的管理員的組織管理員權限：

```
commadmin admin remove -D chris -n sesta.com -w bolton -l admin5 -d test.com
```

commadmin admin search

commadmin admin search 指令搜尋並顯示網域的特定或全部組織管理員。

語法

```
commadmin admin search -D login -n domain -w password [-l login] [-d domain]
```

選項

以下選項是必要的：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。
`-n` *domain*	使用 `-D` 選項指定的使用者所在的網域。
`-w` *password*	使用 `-D` 選項指定的使用者的密碼。

以下選項是非必要的：

選項	說明
`-l` *login*	搜尋的組織管理員的使用者 ID。如果未指定 `-l`，或使用萬用字元運算子 (`-l\\*` 或 `-l '*'`) 指定 `-l`，則顯示網域的所有組織管理員。
`-d` *domain*	搜尋擁有指定網域組織管理員權限的使用者。如果未指定 `-d`，則使用由 `-n` 指定的網域。

範例

若要搜尋 `test.com` 網域的所有組織管理員，請執行以下指令：

```
commadmin admin search -D chris -n sesta.com -w bolton -d test.com
```

commadmin domain create

`commadmin domain create` 指令可在 Access Manager 上建立單一網域。若要建立多個網域，請使用 `-i` 選項。

語法

`commadmin domain create -D` *login* `-d` *domain name* `-n` *domain* `-w` *password* `[-A [+]` *attributename*`:`*value*`] [-h] [-?] [-i` *inputfile*`] [-o` *organization RDN*`] [-p` *AM port*`] [-s] [-v] [-V] [-X` *AM host*`] [-S mail -H` *preferred mailhost*`] [-S cal [-B` *backend calendar data server*`] [-C` *searchable domains*`] [-g` *access control string*`] [-P` *propertyname* `[`*value*`]] [-R` *right* `[:`*value*`]] [-T` *calendar time zone string*`]]`

選項

以下選項是必要的：

選項	說明
`-D` *login*	頂層管理員的使用者 ID。
`-d` *domain name*	將建立之網域的 DNS 網域名稱。
`-n` *domain*	頂層管理員所在的網域。
`-w` *password*	頂層管理員的密碼。

以下選項是非必要的：

選項	說明
`-A` [+]*attributename*:*value*	要修改的屬性。*attributename* 在 LDAP 模式中定義，指定的 *value* 將替代目錄中此屬性的任意或所有目前值。重複此選項可同時修改多個屬性，或爲同一屬性指定多個值。 *attributename* 前面的「+」指示將該值增加至目前屬性清單。 如果未指定動作值 (+)，則預設動作爲增加現有值。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-o` *organization RDN*	指定網域的組織 RDN。例如，`o=varrius.florizel.com`。 如果未指定此選項，則在 `osi suffix` 下建立組織，`o=`網域名稱爲 `o=osiSuffix`。
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

選項	說明
-S *service*	指定要增加至網域的服務。 *service* 值可以爲一個服務或多個服務。有效的 *service* 值爲 mail 和 cal。這些值大小寫不須相符。 如果指定 -S mail 選項，則必須指定 -H 選項。 可以以逗號分隔的清單列出。 例如： -S mail,cal 根據 Identity Sever 配置檔案中的特定服務定義值，使用提到的服務建立網域。
只有在指定 -S mail 選項時，才允許以下選項：	
-H *preferred mailhost*	喜好的網域郵件主機。主機必須具有完全合格的主機名稱，如 mailhost.sesta.com。 如果指定 -S mail 選項，則此選項爲必要的。
只有在指定 -S cal 選項時，才允許以下選項：	
-B *backend calendar data server*	指定在網域中指定給使用者或資源的預設後端主機。
-C *searchable domains*	指定查找行事曆或使用者時要搜尋的網域。
-g *access control string*	指定新建立的使用者行事曆之存取控制清單 (ACL)。
-P *propertyname*[:*value*]	設定多值屬性及位元屬性的值。請參閱第 151 頁的 「屬性值」表，以取得屬性、屬性說明及屬性值。
-R *right*[:*value*]	設定行事曆網域屬性 icsAllowRights。該屬性具有點陣圖值。請參閱第 151 頁的 「屬性值」，以取得屬性、屬性值及屬性說明清單。
-T *calendar time zone string*	指定匯入檔案時使用的時區 ID。 請參閱第 153 頁的 「行事曆時區字串」，以取得有效時區字串清單。

範例

若要使用郵件和行事曆服務建立新的網域，請輸入：

```
commadmin domain create -D chris -d florizel.com -n sesta.com -w bolton \
-S mail,cal -H mailhost.sesta.com
```

commadmin domain delete

`commadmin domain delete` 指令將單一托管網域標記爲已從伺服器中刪除。若要將多個托管網域標記爲已刪除，請使用 `-i` 選項。

第 102 頁的 「commadmin domain purge」指令將永久性移除網域。

若要禁止組織管理員使用服務 (如行事曆服務或郵件服務)，請使用 `-S` 選項。此處，`S` 爲大寫。

語法

`commadmin domain delete -D` *login* `-d` *domain name* `-n` *domain* `-w` *password* `[-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-S` *service*`] [-v] [-V] [-X` *AM host*`]`

選項

以下選項是必要的：

選項	說明
`-D` *login*	頂層管理員的使用者 ID。
`-d` *domain name*	要刪除的 DNS 網域名稱。如果未指定 `-d`，則使用由 `-n` 指定的網域。
`-n` *domain*	頂層管理員所在的網域。
`-w` *password*	頂層管理員的密碼。

以下選項是非必要的：

選項	說明
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-S` *service*	將指定的服務狀態屬性值修改爲「已刪除」。 以逗號分隔多個服務。有效的 *service* 值爲 `mail` 和 `cal`。這些值大小寫不須相符。

選項	說明
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

若要刪除現有網域，請執行以下指令：

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com
```

若要從 `florizel.com` 網域中僅刪除郵件服務，請執行以下指令：

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com \
-S mail
```

commadmin domain modify

`commadmin domain modify` 指令可修改單一網域的目錄項目屬性。若要修改多個網域，請使用 `-i` 選項。

語法

`commadmin domain modify -D` *login* `-d` *domain* `-n` *domain* `-w` *password* `[-A [+|-]` *attributename*`:`*value*`] [-h] [?] [-i` *inputfile*`] [-p` *AM port*`]`
`[-s] [-v] [-V] [-X` *AM host*`] [-S mail -H` *preferred mailhost*`] [-S cal [-g` *access string*`]`
`[-C` *cross domain search domains*`] [-B` *backend calendar data server*`]`
`[-P [`*action*`]` *propertyname* `[:` *value*`]] [-R` *propertyname* `[:`*value*`]] [-T` *calendar time zone string*`]]`

選項

以下選項是必要的：

選項	說明
`-D` *login*	頂層管理員的使用者 ID。
`-d` *domain*	要修改的 DNS 網域名稱。如果未指定 `-d`，則使用由 `-n` 指定的網域。
`-n` *domain*	頂層管理員所在的網域。

選項	說明
-w *password*	頂層管理員的密碼。

以下選項是非必要的：

選項	說明
-A [+ | -]*attributename*:*value*	要修改的屬性。*attributename* 在 LDAP 模式下定義，其值可替代目錄中此屬性的任意或所有現有值。重複此選項可同時修改多個屬性，或爲同一屬性指定多個值。 *attributename* 前面的「+」指示將該值增加至目前屬性清單。「-」指示移除值。 如果使用「-」，則在指令行上指定指令時，必須在指令前加兩個反斜線。如果該選項在輸入檔案中提供，則必須在「-」符號前加一個反斜線。 如果未指定動作值 (+ 或 -)，則預設動作將替代現有值。
-h、-?	顯示指令用法語法。
-i *inputfile*	參閱檔案而非指令行中的指令資訊。
-p *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
-s	使用 SSL (安全通訊端層) 連線 Access Manager。
-v	啓用除錯輸出。
-V	顯示有關公用程式及其版本的資訊。
-X *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。
-S *service*	修改期間將指定的服務增加至網域。 有效的 *service* 值爲 mail 和 cal。這些值大小寫不須相符。 用逗號將使用 -S 選項列出的服務分隔。 如果指定 -S mail，則必須指定 -H 選項。
增加服務時，只有在指定 -S mail 選項時，才允許以下選項：	
-H *preferred mailhost*	喜好的網域郵件主機。 如果指定了 -S mail 選項，則此選項爲必要的。

選項	說明
增加服務時，只有在指定 `-S cal` 選項時，才允許以下選項：	
`-B` *backend calendar data server*	指定給網域中的使用者或資源的預設後端主機。
`-C` *cross domain search domains*	指定查找行事曆或使用者時要搜尋的網域。
`-g` *access string*	指定新建立的使用者行事曆之存取控制清單 (ACL)。
`-P` [*action*]*propertyname* [:*value*]	設定多值屬性及位元屬性的值。請參閱第 151 頁的 「屬性值」表，以取得 *propertyname* 說明及其值。
`-T` *calendar time zone string*	匯入檔案時使用的時區 ID。 請參閱第 153 頁的 「行事曆時區字串」，以取得有效時區字串清單。
`-R` *propertyname*[:*value*]	設定行事曆網域屬性 `icsAllowRights`。該屬性具有點陣圖值。請參閱第 151 頁的 「屬性值」，以取得特性名稱、特性值以及特性說明清單。

範例

若要修改現有網域，請執行以下指令：

```
commadmin domain modify -D chris -w bolton -n sesta.com -d varrius.com \
-A preferredmailhost:test.siroe.com
```

commadmin domain purge

`commadmin domain purge` 指令可永久性移除已標記爲可移除的所有項目或項目之服務。這可以包含網域、使用者、群組及資源。

請使用 `commadmin domain purge` 指令，移除其刪除時間已超過指定寬限期的所有項目，以進行定期維護作業。

可以透過手動呼叫指令隨時執行清除。

呼叫指令時，會搜尋目錄並建立網域清單，該目錄項目包含標記爲刪除時間超過指定的寬限期的網域。寬限期的預設值設定爲 5 天。

如果指定 `-d*` 選項，則會搜尋所有網域中標記爲已刪除的使用者及網域。標記爲已刪除的使用者將從其網域中清除，但是不會清除該網域，除非其也標記爲已刪除。如果網域標記爲已刪除，則將一起清除該網域及其所有使用者。

服務標記爲已刪除後，必須先執行可移除資源 (如電子信箱或行事曆) 的公用程式，才能從目錄中清除該服務。對於郵件服務，該程式爲 `msuserpurge`。請參閱「Sun Java System Messaging Server Administration Reference」，以取得有關 `msuserpurge` 公用程式的資訊。對於行事曆服務，該程式爲 `csclean`。請參閱「 Sun Java System Calendar Server Administration Guide」，以取得有關 `csclean` 公用程式的資訊。

備註 – `commadmin domain purge` 指令必須由頂層管理員執行。

語法

```
commadmin domain purge -D login -n domain -w password -d domain [-g grace] [-h] [-?]
[-i inputfile] [-p AM port] [-s] [-S service] [-v] [-V] [-X AM host]
```

選項

以下選項是必要的：

選項	說明
`-D` *login*	頂層管理員的使用者 ID。
`-n` *domain*	頂層管理員所在的網域。
`-w` *password*	頂層管理員的密碼。
`-d` *domain*	清除指定的網域。* 運算子 (`-d*`) 可以用於搜尋式樣。

以下選項是非必要的：

選項	說明
`-g` *grace*	網域清除之前的寬限期 (以天爲單位)。不會刪除標記爲刪除時間短於 *grace* 天的網域。0 指示立即清除。預設值爲 5 天。永遠不能變更預設值。只能使用 `commadmin domain purge` 指令中的 `-g` (**寬限期**) 選項變更寬限期。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-S` *service*	從網域中移除服務相關的物件類別和屬性。如果網域包含使用者和資源，則將從目錄中移除這些使用者和資源的特定服務資料。 用逗號 (,) 分隔符將服務清單分隔。 有效的 *service* 值爲 `mail` 和 `cal`。這些值大小寫不須相符。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。

選項	說明
-v	啓用除錯輸出。
-V	顯示有關公用程式及其版本的資訊。
-X *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

在以下範例中，將清除 siroe.com 網域，並移除其中的所有項目：

```
commadmin domain purge -D chris -d siroe.com -n sesta.com -w bolton
```

commadmin domain search

commadmin domain search 指令可取得與單一網域相關的所有目錄特性。若要取得多個網域的所有目錄特性，請使用 -i 選項。在此指令中指定 - S 時，將僅顯示具有使用中指定服務的網域。

語法

```
commadmin domain search -D login -n domain -w password [-d domain] [-h] [-?]
[-i inputfile] [-p AM port] [-s] [-S service] [-t Search Template] [-v] [-V] [-X AM host]
```

選項

以下選項是必要的：

選項	說明
-D *login*	有權執行此指令的使用者之使用者 ID。
-n *domain*	使用 -D 選項指定的使用者所在的網域。
-w *password*	使用 -D 選項指定的使用者的密碼。

以下選項是非必要的：

選項	說明
`-d` *domain*	搜尋此網域。如果未指定 `-d`，或指定了 `-d*`，則將顯示所有網域。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-S` *service*	指定要在使用中網域中搜尋的服務。 *service* 值可以爲一個服務或多個服務。有效的 *service* 值爲 `mail` 和 `cal`。這些值大小寫不須相符。 用逗號 (,) 分隔符將服務清單分隔。 例如： `-S mail,cal`
`-t` *Search template*	指定要使用的搜尋範本名稱，而非預設搜尋範本名稱。搜尋後將僅顯示使用中網域。
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

commadmin group create

`commadmin group create` 指令可將單一群組增加至 Access Manager。若要建立多個群組，請使用 `-i` 選項。

如果建立的群組中無成員，則依預設，該群組爲靜態群組。

備註 – 群組無法同時包含靜態和動態成員。

電子郵件發行清單是一種群組類型。郵件傳送至群組位址時，Access Manager 會將該郵件傳送給群組中的所有成員。

語法

```
commadmin group create -D login -G groupname -n domain -w password [-A [+]
attributename:value] [-d domain] [-f ldap-filter] [-h] [-?] [-i inputfile]
[-m internal-member] [-p AM port] [-s] [-v] [-V] [-X AM host] [-S service
[-H mailhost] [-E email] [-M external-member] [-o owner]
[-rs moderator]]
```

選項

以下選項是必要的：

選項	說明
-D *login*	有權執行此指令的使用者之使用者 ID。
-n *domain*	由 -D 選項指定的使用者所在的網域。
-G *groupname*	群組名稱 (例如 mktg-list)。
-w *password*	由 -D 選項指定的使用者密碼。

以下選項是非必要的：

選項	說明
-A [+]*attributename*:*value*	要修改的屬性。*attributename* 在 LDAP 模式中定義，*value* 將替代目錄中此屬性的任意和所有目前值。重複此選項可同時修改多個屬性，或爲同一屬性指定多個值。 *attributename* 前面的「+」指示將該值增加至目前屬性清單。
-d *domain*	群組完全合格的網域名稱 (例如 varrius.com)。預設爲本地網域。如果未指定 -d，則使用由 -n 指定的網域。
-f *ldap-filter*	建立動態群組。 透過指定屬性或屬性組合，設定 LDAP 篩選器。 可以指定多個 -f 指令來定義多個群組成員 LDAP 篩選器。
-h、-?	顯示指令用法語法。
-i *inputfile*	參閱檔案而非指令行中的指令資訊。
-m *internal -member*	增加至此群組的內部成員之使用者 ID。若要增加多個成員，請使用多個 -m 選項。 應使用此選項建立靜態群組。

選項	說明
-p *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
-X *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。
-s	使用 SSL (安全通訊端層) 連線 Access Manager。
-v	啓用除錯輸出。
-V	顯示有關公用程式及其版本的資訊。
-S *service*	指定要增加至群組的服務。 *service* 值可以爲一個服務或多個服務。有效的服務值爲 mail 和 cal。這些值大小寫不須相符。 用逗號 (,) 分隔符將服務清單分隔。 例如： -S mail,cal
只有在指定 -S mail 選項時，才允許以下選項：	
-H *mailhost*	此群組回應的郵件主機 (如 mailhost.varrius.com)。預設爲本地郵件主機。
-E *email*	群組的電子郵件位址。
-M *external-member*	增加至此群組的外部成員之使用者 ID。若要增加多個成員，請使用多個 -M 選項。
-o *owner*	群組所有者的電子郵件位址。所有者爲負責發行清單的個人。 所有者可以增加或刪除發行清單成員。
-r *moderator*	管理者的電子郵件位址。

範例

若要在網域 sesta.com 中建立群組 testgroup，請執行以下指令：

```
commadmin group create -D chris -n sesta.com -w bolton -G testgroup \
-d sesta.com -m lorca@sesta.com -S mail -M achiko@varrius.com
```

commadmin group delete

commadmin group delete 指令可將單一群組標記爲已刪除。若要將多個群組標記爲已刪除，請使用 -i 選項。

若要停用群組使用的服務 (例如 Calendar Server 或 Messaging Server)，請使用 `-S` 選項。此處，`S` 爲大寫。

備註 – 若要永久性移除群組，必須執行以下指令：第 102 頁的 「commadmin domain purge」 。

語法

`commadmin group delete -D` *login* `-G` *groupname* `-n` *domain* `-w` *password* `[-d` *domain*`] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-S` *service*`] [-v] [-V] [-X` *AM host*`]`

選項

以下是必要的選項：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。
`-G` *groupname*	要標記爲已刪除的群組之名稱。例如，`mktg-list`。
`-n` *domain*	由 `-D` 選項指定的使用者所在的網域。
`-w` *password*	由 `-D` 選項指定的使用者密碼。

以下是非必要的選項：

選項	說明
`-d` *domain*	群組所在的網域。如果未指定 `-d`，則使用由 `-n` 選項指定的網域。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-S` *service*	將指定的服務狀態屬性值修改爲「已刪除」。 用逗號將使用 `-S` 選項列出的服務分隔。有效的 *service* 值爲 `mail` 和 `cal`。這些值大小寫不須相符。

選項	說明
-v	啓用除錯輸出。
-V	顯示有關公用程式及其版本的資訊。
-X *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

以下範例將群組 testgroup@varrius.com 標記爲已刪除：

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com
```

以下範例將 testgroup@varrius.com 的郵件服務標記爲已刪除：

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com -S mail
```

commadmin group modify

commadmin group modify 指令可變更 Access Manager 中單一群組的屬性。若要變更多個群組的屬性，請使用 -i 選項。

郵件收信人清單是一種群組類型。郵件傳送至群組位址時，Access Manager 會將該郵件傳送給群組中的所有成員。

語法

```
commadmin group modify -D login -G groupname -n domain -w password [-A [+|-]
attributename:value] [-d domain] [-f [action] ldap-filter] [-h] [-?]
[-i inputfile] [-m [+|-] internal-member] [-p AM port] [-s] [-v] [-V]
[-X AM host] [-S mail [-o owner] [-E email] [-H mailhost] [-M external-member]
[-r moderator]]
```

選項

以下是必要的選項：

選項	說明
-D *login*	有權執行此指令的使用者之使用者 ID。

選項	說明
-G *groupname*	要修改的群組之名稱。例如，mktg-list。
-n *domain*	由 -D 選項指定的使用者所在的網域。
-w *password*	由 -D 選項指定的使用者密碼。

以下是非必要的選項：

選項	說明
-A [+ | -]*attributename*:*value*	要修改的屬性。*attributename* 在 LDAP 模式下定義，其值可替代目錄中此屬性的任意或所有現有值。重複此選項可同時修改多個屬性，或爲同一屬性指定多個值。 *attributename* 前面的「+」指示將該值增加至目前屬性清單。「-」指示移除值。如果使用「-」，則在指令行上指定指令時，必須在指令前加兩個反斜線，或者用引號引起來。如果該選項在輸入檔案中提供，則必須在「-」符號前加一個反斜線。
-d *domain*	群組所在的網域。如果未指定 -d，則使用由 -n 選項指定的網域。
- f [*action*] *ldap-filter*	指示是否將 lDAP 篩選器增加至群組或從群組中將其移除 *ldap-filter* 前面的「+」指示其將被增加至現有篩選器。「-」指示移除該現有篩選器。鍵入 -f-* 以移除所有篩選器。如果使用「-」，則在指令行上指定指令時，必須在指令前加兩個反斜線，或者用引號引起來。 如果未指定 *action*，則依預設，增加該篩選器 (假設尚未存在)。否則，會顯示錯誤訊息。
-h、-?	顯示指令用法語法。
-i *inputfile*	參閱檔案而非指令行中的指令資訊。
-m [*action*] *internal -member*	指示是否增加或移除內部成員。 內部 *-member* 的值爲郵件位址或使用者 ID。 *action* 值爲： +，向現有內部成員清單增加成員。 -，從現有內部成員清單中移除成員。如果使用「-」，則在指令行上指定指令時，必須在指令前加兩個反斜線，或者用引號引起來。 -m-* 可移除所有內部成員。
-p *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。

選項	說明
-s	使用 SSL (安全通訊端層) 連線 Access Manager。
-v	啓用除錯輸出。
-V	顯示有關公用程式及其版本的資訊。
-X *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。
-S mail	驗證完郵件服務是否存在後，在修改期間向群組增加郵件服務。如果服務已存在，則會顯示錯誤訊息。 -S 的唯一有效值爲 mail。
只有在指定 -S mail 選項時，才允許以下選項：	
-o *owner*	群組所有者的電子郵件位址。所有者爲負責發行清單的個人。 所有者可以增加或刪除發行清單成員。
-E *email*	群組的電子郵件位址。
-H *mailhost*	群組的郵件主機。預設爲本地郵件主機。
-M *external -member*	增加外部成員。 *external-member* 的值爲使用者郵件位址。
-r *moderator*	管理者的使用者 ID。如果該管理者位於其他網域中，則鍵入電子郵件位址。 必須使用此選項指定 -S mail 選項。

範例

若要從網域 varrius.com 的群組 testgroup 中移除內部成員 (jsmith)，請執行以下指令：

```
commadmin group modify -D chris -d varrius.com -G testgroup -n sesta.com \
-w bolton -m \\-jsmith
```

commadmin group search

commadmin group search 指令可取得與單一群組相關的所有目錄特性。若要取得多個群組的所有目錄特性，請使用 -i 選項。

語法

`commadmin group search -D` *login* `-n` *domain* `-w` *password* `[-d` *domain*`] [-E` *string*`] [-G` *string*`] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-S` *service*`] [-t` *search template*`] [-v] [-V] [-X` *AM host*`]`

選項

以下選項是必要的：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。
`-n` *domain*	由 `-D` 選項指定的使用者所在的網域。
`-w` *password*	由 `-D` 選項指定的使用者密碼。

以下選項是非必要的：

選項	說明
`-d` *domain*	要搜尋的群組所在的網域。如果未指定 `-d`，則將搜尋所有網域。
`-E` *string*	群組的電子郵件位址。可以在字串的任何部位使用萬用字元運算子 (*)。
`-G` *string*	要搜尋的群組之名稱。例如，`mktg-list`。如果未指定 `-G`，則顯示由 `-d` 指定的網域中的所有群組。可以在字串的任何部位使用萬用字元運算子 (*)。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-p` *AM port*	指定 IS 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-S` *service*	指定要搜尋的服務。 *service* 的唯一有效值爲 `mail`。此值大小寫不須相符。 例如： `-S mail` 僅顯示包含使用中服務的群組。

選項	說明
`-t` *Search Template*	指定要使用的搜尋範本名稱，而非預設搜尋範本名稱。這是定義搜尋篩選器目錄中的項目。僅搜尋使用中群組。
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

若要在 `siroe.com` 網域中搜尋名爲 `developers` 的群組，請執行以下指令：

```
commadmin group search -D chris -n sesta.com -w password -G developers \
-d siroe.com
```

commadmin resource create

`commadmin resource create` 指令可建立資源目錄項目。

如需有關建立資源的說明，請參閱第 115 頁的 「建立資源」。

語法

`commadmin resource create -D` *login* `-n` *domain* `-w` *password* `-u` *identifier* `-N` *name* `-o` *owner* `[-c` *calendar identifier*`] [-A [+]` *attributename*`:`*value*`] [-C` *DWPHost*`] [-d` *domainname* `] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-T` *time zone*`] [-v] [-V] [-X` *AM host*`]`

選項

以下選項是必要的：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。
`-n` *domain*	使用 `-D` 選項指定的使用者所在的網域。
`-w` *password*	使用 `-D` 選項指定的使用者密碼。

選項	說明
`-u` *identifier*	資源的唯一識別碼。 此 *identifier* 值應在網域名稱空間，或行事曆模式下行事曆管理的所有使用者和資源中是唯一的。
`-N` *name*	用於顯示行事曆 GUI 中的資源之易於識別的名稱。
`-o` *owner*	資源的所有者。此使用者 ID 必須位於在其中建立資源的網域中。
`-c` *calendar identifier*	此資源行事曆的識別碼。 此識別碼值應在由 Calendar Server 管理的所有行事曆中爲唯一值。

以下選項是非必要的：

選項	說明
`-A` [+] *attributename*:*value*	要修改的屬性。*attributename* 在 LDAP 模式中定義，*value* 將替代目錄中此屬性的任意和所有目前值。重複此選項可同時修改多個屬性，或爲同一屬性指定多個值。 *attributename* 前面的「+」指示將該值增加至目前屬性清單。
`-C` *DWPHost*	託管此使用者行事曆的後端行事曆伺服器之 DNS 名稱。 如果未指定後端行事曆伺服器的 DNS 名稱，則儲存於伺服器 ics.conf 檔案中的值將用做預設值。
`-d` *domain name*	資源所在的網域。如果未指定 `-d`，則使用由 `-n` 指定的網域。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-T` *time zone*	用於顯示行事曆使用者介面中的資源行事曆之時區。 請參閱第 153 頁的 「行事曆時區字串」，以取得有效時區字串清單。
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

若要在網域 varrius.com 下的行事曆 cal.siroe.com 中建立名爲 peter 的資源，請執行以下指令：

```
commadmin resource create -D chris -n sesta.com -w bolton -o ownerid \
-d varrius.com -u id -c calid -N peter -C cal.siroe.com
```

建立資源

資源由兩個資料說明組成：Calendar Server 資料庫中的目錄項目和行事曆。目錄項目具有屬性 icsCalendar，其值爲與資源相關的行事曆之名稱。

可以使用以下方法之一，建立具有這兩個資料說明的資源：

- 使用 csresource 公用程式本身。csresource 公用程式可建立目錄項目和行事曆。

  但是，僅當目錄在 Schema 1 環境中且您未使用 Access Manager 時，才建議使用 csresource 同時建立目錄項目和行事曆。

- 使用 commadmin resource create 建立目錄項目，使用 csresource 公用程式建立行事曆。例如：

  使用 commadmin resource create 建立目錄項目：

  ```
  commadmin resource create -D amadmin -w ampassword -n blink.sesta.com
   -X blink -p 5555 -d varrius.com -o test1 -u resourceOne
   -N firstResource -c resourceOneCalendar
  ```

  目錄項目如下：

  ```
  dn: uid=resourceONE,ou=People,o=varrius,o=domainroot
  uid: resrouceONE
  objectClass: icsCalendarResource
  objectClass: top
  cn: firstResource
  icsStatus: active
  icsCalendar: test1@varrius.com:resourceOne
  ```

  使用 csresource 建立行事曆。

備註：呼叫 csresource 中的 create 指令時，輸入的資源名稱值必須與用於 commadmin resource create 中 -u 選項的值相同。

現在即可以以任何使用者身份登入，並邀請資源參加事件。

如需有關 csresource 公用程式的詳細說明，請參閱「Sun Java System Calendar Server Administration Guide」中的「Calendar Server Command-Line Utilities」。

commadmin resource delete

commadmin resource delete 指令可將資源標記爲已刪除。

備註 – 若要永久性移除資源，請執行第 102 頁的 「commadmin domain purge」。

語法

```
commadmin resource delete -D login -u identifier -n domain -w password [-d domainname]
[-h] [-?] [-i inputfile] [-p AM port] [-s] [-v] [-V] [-X AM host]
```

選項

以下選項是必要的：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。
`-n` *domain*	使用 `-D` 選項指定的使用者所在的網域。
`-w` *password*	使用 `-D` 選項指定的使用者密碼。
`-u` *identifier*	資源的唯一識別碼。

以下選項是非必要的：

選項	說明
`-d` *domainname*	資源所在的網域。如果未指定 `-d`，則使用由 `-n` 指定的網域。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

若要將資源標記爲已刪除，請執行以下指令：

```
commadmin resource delete -D chris -n sesta.com -w bolton -u bill023
```

commadmin resource modify

`commadmin resource modify` 指令可修改資源。

語法

`commadmin resource modify -D` *login* `-n` *domain* `-w` *password* `-u` *identifier* `[-A [+|-]` *attributename*`:`*value*`] [-d` *domainname* `] [-h] [-?] [-i` *inputfile*`] [-N` *name*`] [-p` *AM port*`] [-s] [-T` *time zone*`] [-v] [-V] [-X s`*AM host*`]`

選項

以下選項是必要的：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。
`-n` *domain*	使用 `-D` 選項指定的使用者所在的網域。
`-w` *password*	使用 `-D` 選項指定的使用者密碼。
`-u` *identifier*	資源的唯一識別碼。

以下選項是非必要的：

選項	說明
`-A [+ | -]`*attributename*:*value*	要修改的屬性。*attributename* 在 LDAP 模式下定義，其值可替代目錄中此屬性的任意或所有現有值。重複此選項可同時修改多個屬性，或爲同一屬性指定多個值。 *attributename* 前面的「+」指示將該值增加至目前屬性清單。「-」指示移除值。 如果使用「-」，則在指令行上指定指令時，必須在指令前加兩個反斜線。如果該選項在輸入檔案中提供，則必須在「-」符號前加一個反斜線。
`-d` *domainname*	資源所在的網域。如果未指定 `-d`，則使用由 `-n` 指定的網域。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-N` *name*	用於顯示行事曆使用者介面中的資源之一般名稱。

選項	說明
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-T` *time zone*	用於顯示行事曆 GUI 中的資源行事曆之時區。 請參閱第 153 頁的 「行事曆時區字串」，以取得有效時區字串清單。
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

若要修改唯一識別碼爲 `bill023` 的資源，使其新的一般名稱爲 `bjones`，請執行以下指令：

```
commadmin resource modify -D chris -n sesta.com -w bolton -d test.com \
-u bill023 -N bjones
```

commadmin resource search

`commadmin resource search` 指令可搜尋資源。

語法

```
commadmin resource search -D login -n domain -w password [-d domain] [-h] [-?]
[-i inputfile] [-N string] [-p AM port] [-s] [-t Search Template] [-u string]
[-V] [-v] [-X AM host]
```

選項

以下選項是必要的：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。

選項	說明
-n *domain*	使用 -D 選項指定的使用者所在的網域。
-w *password*	使用 -D 選項指定的使用者密碼。

以下選項是非必要的：

選項	說明
-d *domain*	資源所在的網域。僅在網域中執行搜尋。如果未指定 -d，或指定了 -d*，則將顯示所有網域。
-h、-?	顯示指令用法語法。
-i *inputfile*	參閱檔案而非指令行中的指令資訊。
-N *string*	輸入資源的一般名稱。可以在字串的任何部位使用萬用字元運算子 (*)。
-p *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
-s	使用 SSL (安全通訊端層) 連線 Access Manager。
-t *Search Template*	指定要使用的搜尋範本名稱，而非預設搜尋範本名稱。這是定義搜尋篩選器目錄中的項目。僅搜尋使用中資源。
-u *string*	指定的資源識別碼對於網域名稱空間，或由行事曆管理的所有使用者和資源必須是唯一的。 可以在字串的任何部位使用萬用字元運算子 (*)。 如果未指定該識別碼，或指定了 -l*，則將在搜尋期間顯示所有資源。
-v	啓用除錯輸出。
-V	顯示有關公用程式及其版本的資訊。
-X *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

若要在網域 sesta.com 中搜尋資源 arabella，請執行以下指令：

```
commadmin resource search -D serviceadmin -w serviceadmin -n sesta.com \s
-d sesta.com -u arabella
```

commadmin user create

`commadmin user create` 指令可在 Access Manager 系統中建立單一使用者。若要建立多個使用者，請使用 `-i` 選項。

語法

`commadmin user create -D` *login* `-F` *firstname* `-n` *domain* `-L` *lastname* `-l` *userid* `-w` *password* `-W` *password* `[-A [+]` *attributename*`:`*value*`] [-d` *domain*`] [-I` *initial*`] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-v] [-V] [-X` *AM host*`] [-S mail [-E` *email*`] [-H` *mailhost*`]] [-S cal [-B` *DWPHost*`] [-E` *email*`] [-k` *calid_type*`] [-J` *First Day of Week*`] [-T` *time zone*`]`

選項

以下選項是必要的：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。
`-F` *firstname*	使用者的名字必須是沒有空格的單個詞。
`-n` *domain*	使用 `-D` 選項指定的使用者所在的網域。
`-l` *userid*	使用者的登入名稱。
`-w` *password*	使用 `-D` 選項指定的使用者密碼。
`-W` *password*	要建立的使用者之密碼。 也可以透過文字檔 *password*`.txt` 指定 *password*。
`-L` *lastname*	使用者的姓氏。

以下選項是非必要的：

選項	說明
`-A [+ ]`*attributename*:*value*	要修改的屬性。*attributename* 在 LDAP 模式中定義，*value* 將替代目錄中此屬性的任意和所有目前值。重複此選項可同時修改多個屬性，或爲同一屬性指定多個值。 *attributename* 前面的「+」指示將該值增加至目前屬性清單。
`-d` *domain*	使用者所在的網域。如果未指定 `-d`，則使用由 `-n` 指定的網域。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。

選項	說明
`-I` *initial*	使用者中間名字的首字母。
`-h`、`-?`	顯示指令用法語法。
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。
`-S` *service*	建立期間向使用者增加指定的服務。*service* 值可以爲一個服務或多個服務。有效的 *service* 值爲 `mail` 和 `cal`。這些值大小寫不須相符。 用逗號 (,) 分隔符將服務清單分隔。 例如： `-S mail,cal`
只有在指定 `-S mail` 選項時，才允許以下選項：	
`-E` *emai*l	使用者的電子郵件位址。
`-H` *mailhost*	使用者的郵件主機。
只有在指定 `-S cal` 選項時，才允許以下選項：	
`-B` *DWPHost*	託管使用者行事曆的後端行事曆之 DNS 名稱。
`-E` *email*	行事曆使用者的電子郵件位址。
`-J` *First Day of Week*	在行事曆伺服器使用者介面中顯示行事曆時的週的第一天。有效值爲 0-6 (0 爲星期日，1 爲星期一，以此類推)。

選項	說明
-k *calid_type*	指定建立的行事曆 ID 的類型。接受的值爲 legacy 和 hosted。如果指定了 -k legacy，則僅使用行事曆 ID (例如 jsmith)。如果指定了 -k hosted，則使用行事曆 ID 和網域 (例如 jsmith@sesta.com)。 如果未指定 -k 選項，則依預設使用行事曆 ID 和網域 (hosted)。 如果未指定 -k 選項，則可以設定建立的行事曆 ID 類型值。若要執行此作業，請將以下參數增加至 resource.properties 檔案： switch-caltype=*value* 其中，*value* 爲「hosted」|「legacy」。 resource.properties 檔案位於以下目錄中： *da_base*/data/WEB-INF/classes/sun/comm/cli/ \ server/servlet/resource.properties
-T *time zone*	使用者行事曆顯示的時區。 請參閱第 153 頁的 「行事曆時區字串」，以取得有效時區字串清單。

範例

若要建立新使用者 smith，請輸入：

```
commadmin user create -D chris -n sesta.com -w secret -F smith -l john \
-L major -W secret -S mail -H mailhost.siroe.com
```

commadmin user delete

commadmin user delete 指令可將單一使用者標記爲已刪除。若要將多個使用者標記爲已刪除，請使用 -i 選項。

無取消刪除公用程式。但是，在清除寬限期到期且將清除設定爲對項目執行之前，可以隨時使用 ldapmodify 指令將使用者項目的狀態屬性變更爲 active。

▼ 移除使用者

步驟 1. **透過執行 commadmin user delete 指令可將使用者標記為已刪除。**

2. **移除使用者資源。**
   資源可以是電子信箱或行事曆。

對於郵件服務，該程式爲 msuserpurge。請參閱「Sun Java System Messaging Server Administration Reference」，以取得有關 msuserpurge 公用程式的資訊。

對於行事曆服務，該程式爲 csclean。請參閱「 Sun Java System Calendar Server Administration Guide」，以取得有關 csclean 公用程式的資訊。

3. **透過呼叫以下指令可以永久性移除使用者：第 102 頁的 「commadmin domain purge」。**

語法

```
commadmin user delete -D login -n domain -l login name -w password [-d domain] [-h]
[-?] [-i inputfile] [-p AM port] [-s] [-S service] [-v] [-V] [-X AM host]
```

選項

以下選項是必要的：

選項	說明
-D *login*	有權執行此指令的使用者之使用者 ID。
-n *domain*	使用 -D 選項指定的使用者所在的網域。
-w *password*	使用 -D 選項指定的使用者密碼。
-l *userid*	要刪除的使用者之使用者 ID。

以下選項是非必要的：

選項	說明
-d *domain*	使用者所在的網域。如果未指定 -d，則使用由 -n 指定的網域。
-h、-?	顯示指令用法語法。
-i *inputfile*	參閱檔案而非指令行中的指令資訊。
-p *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
-s	使用 SSL (安全通訊端層) 連線 Access Manager。

選項	說明
-S *service*	指定要移除的使用者服務。使用者保持使用中狀態，僅關閉指定的服務。如果未指定 -S，則刪除該使用者。 *service* 值可以爲一個服務或多個服務。有效的 *service* 值爲 mail 和 cal。這些值大小寫不須相符。 用逗號 (,) 分隔符將服務清單分隔。 例如： -S mail,cal
-v	啓用除錯輸出。
-V	顯示有關公用程式及其版本的資訊。
-X *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

若要將現有使用者標記爲已刪除，請執行以下指令：

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith
```

若要僅刪除使用者 smith 的郵件服務，請執行以下指令：

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith -S mail
```

commadmin user modify

commadmin user modify 指令可修改單一使用者的目錄項目屬性。若要修改多個使用者，請使用 -i 選項。

語法

commadmin user modify -D *login* -n *domain* -l *userid* -w *password* [-A [+|-] *attributename*:*value*] [-d *domain*] [-h] [-?] [-i *inputfile*] [-p *AM port*] [-s] [-v] [-V] [-X *AM host*] [-S mail -H *mailhost* [-E *email*]] [-S cal [-B *DWPHost*] [-E *email*] [-k *calid_type*] [-J *First Day of Week*] [-T *time zone*]]

選項

以下選項是必要的：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。
`-n` *domain*	使用 `-D` 選項指定的使用者所在的網域。
`-w` *password*	使用 `-D` 選項指定的使用者密碼。
`-l` *userid*	使用者的登入 ID。

以下選項是非必要的：

選項	說明
`-A` [`+` | `-`]*attributename*:*value*	要修改的屬性。*attributename* 在 LDAP 模式下定義，其值可替代目錄中此屬性的任意或所有現有值。重複此選項可同時修改多個屬性，或爲同一屬性指定多個值。 *attributename* 前面的「+」指示將該值增加至目前屬性清單。 「-」指示移除值。 如果使用「-」，則在指令行上指定指令時，必須在指令前加兩個反斜線。如果該選項在輸入檔案中提供，則必須在「-」符號前加一個反斜線。
`-d` *domain*	使用者或群組所在的網域。如果未指定 `-d`，則使用由 `-n` 指定的網域。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-p` *AM port*	指定 Access Manager 要偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

選項	說明
-S *service*	驗證是否提供使用者使用 -S 選項指定的服務後，向使用者增加指定的服務。如果已經向使用者提供了該服務，則會顯示錯誤訊息。 *services* 值可以爲一個服務或多個服務。有效的 *service* 值爲 mail 和 cal。這些值大小寫不須相符。 用逗號 (,) 分隔符將服務清單分隔。 例如： -S mail,cal
只有在指定 -S mail 選項時，才允許以下選項：	
-E *email*	指定使用者的電子郵件位址。
-H *mailhost*	使用者的郵件主機。 如果指定 -S mail 選項，則此選項爲必要的。
只有在指定 -S cal 選項時，才允許以下選項：	
-B *DWPHost*	指定託管此使用者行事曆的後端行事曆伺服器之 DNS 名稱。 備註只能增加、不能修改 (如果已存在) 此屬性。
-E *email*	指定行事曆使用者的電子郵件位址。
-J *First Day of Week*	在行事曆伺服器使用者介面中顯示行事曆時的週的第一天。有效值爲 0-6 (0 爲星期日，1 爲星期一，以此類推)。
-k *calid_type*	指定建立的行事曆 ID 的類型 (增加行事曆服務時)。接受的值爲 legacy 和 hosted。如果指定了 -k legacy，則僅使用行事曆 ID (例如 jsmith)。如果指定了 -k hosted，則使用行事曆 ID 和網域 (例如 jsmith@sesta.com)。 如果未指定 -k 選項，則依預設使用行事曆 ID 和網域 (hosted)。 如果未指定 -k 選項，則可以設定建立的行事曆 ID 類型值。若要執行此作業，請將以下參數增加至 resource.properties 檔案： switch-caltype=*value* 其中，*value* 爲「hosted」|「legacy」。 resource.properties 檔案位於以下目錄中： *da_base*/data/WEB-INF/classes/sun/comm/cli/ \ server/servlet/resource.properties

選項	說明
`-T` *time zone*	使用者行事曆將顯示的時區爲此時區。 請參閱第 153 頁的 「行事曆時區字串」，以取得有效時區字串清單。

範例

以下範例可爲使用者 `smith` 增加郵件服務：

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A description:"new description" -S mail -H mailhost.siroe.com
```

在以下範例中，可爲使用者 `smith` 增加郵件轉寄位址：

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A +mailforwardingaddress:tsmith@siroe.com
```

commadmin user search

`commadmin user search` 指令可取得與單一使用者相關的所有目錄特性。若要取得多個使用者的所有目錄特性，請使用 `-i` 選項。搜尋後將僅顯示使用中的使用者。

語法

`commadmin user search -D` *login* `-n` *domain* `-w` *password* `[-d` *domain*`] [-E` *string*`] [-F` *string*`] [-h] [-?] [-i` *inputfile*`] [-L` *string*`] [-l` *string*`] [-p` *AM port*`] [-s] [-S` *service*`] [-t` *Search Template*`] [-v] [-V] [-X` *AM host*`]`

選項

以下選項是必要的：

選項	說明
`-D` *login*	有權執行此指令的使用者之使用者 ID。
`-n` *domain*	使用 `-D` 選項指定的使用者所在的網域。
`-w` *password*	使用 `-D` 選項指定的使用者密碼。

以下選項是非必要的：

選項	說明
`-d` *domain*	使用者所在的網域。僅在指定的網域中搜尋該使用者。 如果未指定 `-d`，則搜尋所有網域。
`-E` *string*	搜尋使用者的郵件位址。可以在字串的任何部位使用萬用字元運算子 (*)。
`-F` *string*	搜尋使用者的名字。可以在字串的任何部位使用萬用字元運算子 (*)。
`-h`、`-?`	顯示指令用法語法。
`-i` *inputfile*	參閱檔案而非指令行中的指令資訊。
`-L` *string*	搜尋使用者的姓氏。可以在字串的任何部位使用萬用字元運算子 (*)。
`-l` *string*	搜尋使用者的登入名稱。可以在字串的任何部位使用萬用字元運算子 (*)。
`-p` *AM port*	使用此選項指定 Access Manager 偵聽的替代 TCP 連接埠。如果未指定，則使用預設 *AM port*；或者如果在安裝時未配置預設連接埠，則使用連接埠 80。
`-s`	使用 SSL (安全通訊端層) 連線 Access Manager。
`-S` *service*	指定與使用者搜尋相符的服務。 *services* 值可以爲一個服務或多個服務。有效的 *service* 值爲 `mail` 和 `cal`。這些值大小寫不須相符。 用逗號 (,) 分隔符將服務清單分隔。 例如： `-S mail,cal`
`-t` *Search template*	指定要使用的搜尋範本名稱，而非預設搜尋範本名稱。這是定義搜尋篩選器目錄中的項目。僅搜尋使用中的使用者。
`-v`	啓用除錯輸出。
`-V`	顯示有關公用程式及其版本的資訊。
`-X` *AM host*	指定執行 Access Manager 的主機。如果未指定，則使用預設 *AM host*；或者如果在安裝時未配置預設主機，則使用本地主機。

範例

以下範例可在 `varrius.com` 網域中搜尋使用者：

```
commadmin user search -D chris -w bolton -d varrius.com -n sesta.com
```

附錄 A

服務提供者管理員和服務提供者組織

Delegated Administrator 主控台提供新的管理員角色 (服務提供者管理員 [SPA])，以及可以在目錄中建立的新類型組織。

本附錄說明以下主題：

本附錄說明服務提供者管理員角色和新的組織類型，並說明如何在 Delegated Administrator 中建立它們。

服務提供者管理員

Delegated Administrator 主控台可讓您將管理作業委託給新的角色 (服務提供者管理員 [SPA])，該角色可以建立和管理新類型的從屬組織。

SPA 的權限範圍介於頂層管理員 (TLA) 和組織管理員 (OA) 的權限之間。

使用 SPA，您可以建立三階式管理階層，如第 1 章中的第 24 頁的 「三階式階層」所述。

此第二層級的委託可使對大型 LDAP 目錄支援的大型用戶基底的管理變得容易。例如，ISP 可以爲數以百計或數以千計的小型企業提供服務，其中的每個企業都需要其自己的組織。每天都有許多新的組織應增加至目錄中。

如果您使用兩階式階層，則 TLA 應建立所有這些新組織。現在，TLA 可以將這些作業委託給 SPA。

SPA 可以爲新用戶建立從屬組織，並指定 OA 來管理這些組織中的使用者。

圖 A–1 顯示了三階式組織階層範例的邏輯視圖。

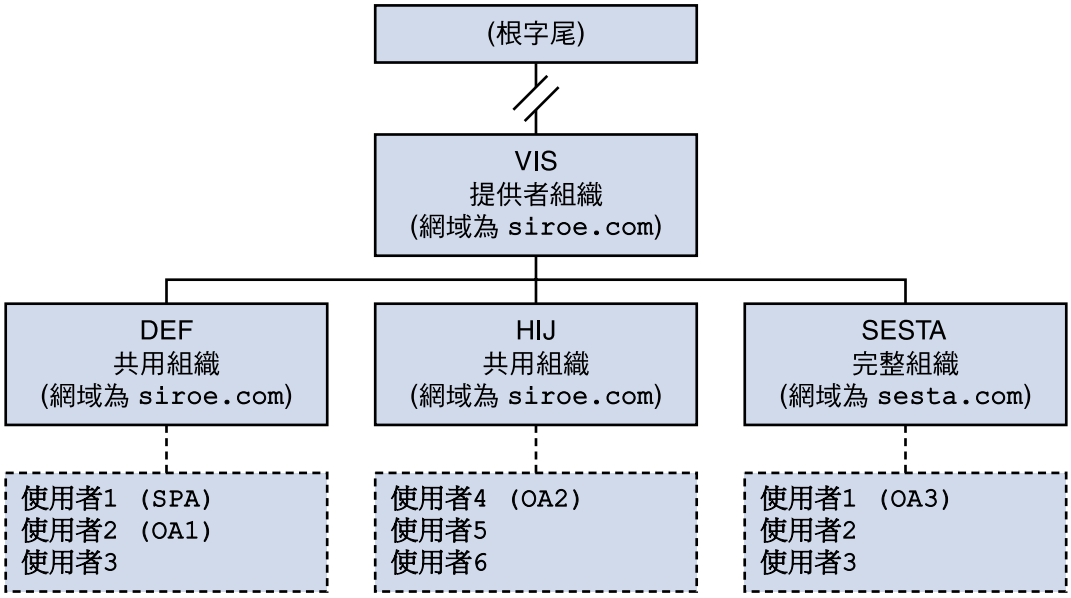

圖 A–1 使用服務提供者管理員的目錄：邏輯視圖

圖 A–1 中的範例顯示了一個提供者組織。然而，目錄可以包含多個提供者組織。

在此範例中，按如下方式委託管理作業：

- SPA 具有管理 VIS 提供者組織及其下所有組織的權限。將 SPA 角色指定給 DEF 組織中的使用者1。
- 名爲 OA1 的組織管理員管理 DEF (一個共用組織)。將此 OA 角色指定給 DEF 組織中的使用者2。
- OA2 管理 HIJ (一個共用組織)。將此 OA 角色指定給 HIJ 組織中的使用者4。
- OA3 管理 SESTA (一個完整組織)。將此 OA 角色指定給 SESTA 組織中的使用者1 。

  SESTA 是完整組織，具有其自己的唯一名稱空間。SESTA (位於 sesta.com 網域中) 中的使用者 1 具有唯一使用者 ID。

如需提供者和從屬組織的定義，請參閱第 132 頁的 「服務提供者管理員管理的組織」。

服務提供者管理員角色

SPA 可執行以下作業：

- 在 SPA 具有管理權限的提供者組織中，建立、刪除和修改共用組織和完整組織。

  在圖 A–1 所示的範例中，VIS 提供者組織的 SPA 可以

    - 修改或刪除 DEF、HIJ 和 SESTA 組織
    - 在 VIS 提供者組織下建立其他組織。
- 建立、刪除和修改提供者組織下任何組織中的使用者。
- 建立、刪除和修改提供者組織下任何組織中的群組。
- 建立、刪除和修改提供者組織下任何組織中的行事曆資源。
- 將 OA 角色指定給使用者。

  例如，在圖 A–1 所示的組織範例中，SPA 可以將 OA 角色指定給 SESTA 組織中的使用者 2。然後，使用者 2 便可以管理 SESTA 組織中的使用者。

  SPA 也可以移除使用者的 OA 角色。
- 將 SPA 角色指定給提供者組織下的其他合法使用者 (以及移除 SPA 角色)。
- 將服務套裝軟體配置給組織。

  如需有關服務套裝軟體的資訊，請參閱第 1 章中第 30 頁的 「服務套裝軟體」。

  SPA 可以爲組織指定特定類型的服務套裝軟體，並確定該組織中可以使用的每種套裝軟體的最大數目。

  例如，SPA 可以指定以下服務套裝軟體：

    - 在 DEF 組織中：

      ```
      1,000 gold packages
      500 platinum packages
      ```

    - 在 HIJ 組織中：

      ```
      2,500 topaz packages
      500 platinum packages
      500 emerald packages
      1,000 ruby packages
      ```

    - 在 SESTA 組織中：

      ```
      2,000 silver packages
      1,500 gold packages
      100 platinum packages
      ```

      SPA 可以使用 Delegated Administrator 主控台執行這些作業。在此發行版本中，Delegated Administrator 公用程式不包含用於執行這些作業的指令選項。

備註 – TLA 可修改或刪除任何現有的共用組織或完整組織。TLA 還可以管理這些組織中的使用者。

TLA 可以透過主控台移除使用者的 SPA 角色，但無法指定 SPA 角色。如需此發行版本的 Delegated Administrator 中的限制清單，請參閱第 132 頁的 「此發行版本的注意事項」。

如需有關 TLA 執行的管理作業的完整說明，請參閱第 1 章中的第 25 頁的 「管理員角色和目錄階層」。

將 SPA 角色指定給使用者

必須將 SPA 角色指定給符合以下條件的組織中的使用者：爲 SPA 而指定，且從屬於 SPA 將管理的提供者組織。

在圖 A–1 所示的範例中，假設您需要爲名爲 VIS 的提供者組織建立 SPA。您可以將 SPA 角色指定給 DEF 組織中的使用者1。

SPA 必須在從屬組織中，因爲提供者組織節點不包含任何使用者。

因此，必須先在提供者組織下至少建立一個組織，然後 SPA 才可對其進行管理。應該指定此組織來保留被指定 SPA 角色的使用者。如需更多資訊，請參閱第 133 頁的 「建立提供者組織和服務提供者管理員」。

此發行版本的注意事項

在此發行版本的 Delegated Administrator 中，您無法使用 Delegated Administrator 主控台或公用程式建立 SPA 或提供者組織。

若要建立 SPA 或提供者組織，您必須手動修改自訂服務提供者範本 `da.provider.skeleton.ldif`。

如需有關使用自訂服務提供者範本執行這些作業的說明，請參閱本附錄後面部分的第 133 頁的 「建立提供者組織和服務提供者管理員」。

服務提供者管理員管理的組織

SPA 可以建立、修改和刪除從屬於 SPA 的提供者組織的以下類型組織：

- 第 133 頁的 「完整組織」
- 第 133 頁的 「共用組織」

接下來的各小節中說明了提供者組織、完整組織和共用組織。

提供者組織

提供者組織是 LDAP 目錄中的節點，邏輯上包含完整組織和共用組織 。提供者組織節點的屬性可讓 SPA 管理從屬組織。

在 LDAP 目錄中，提供者組織必須在郵件網域之下。如需範例，請參閱本附錄後面部分的第 147 頁的 「服務提供者組織資料範例」。

提供者組織不能包含使用者項目。然而，可以在提供者組織下建立的組織中佈建使用者。

提供者組織儲存有關在其下建立的組織的目錄資訊。例如：

- 提供者組織是包含共用組織、完整組織還是同時包含二者
- 在此提供者組織下建立的共用組織可以使用的網域名稱
- 可供此提供者組織下建立的組織使用的服務類別套裝軟體的類型和數目
- 指定爲提供者組織的 SPA 之家的組織。

完整組織

完整組織具有以下特徵：

- 從屬於提供者組織，由 SPA 建立。
- 可以在完整組織中佈建使用者。

  在圖 A–1 所示的範例中，使用者2 屬於 `sesta.com` 網域，且其郵件位址爲 `user2@sesta.com`。
- 完整組織具有自己的網域 (其他組織無法共用該網域)，並且具有自己的唯一名稱空間。

  在圖 A–1 所示的範例中，完整組織 SESTA 的網域名稱爲 `sesta.com`。

共用組織

共用組織具有以下特徵：

- 從屬於提供者組織，由 SPA 建立。
- 可以在共用組織中佈建使用者。

  在圖 A–1 所示的範例中，使用者5 屬於 `siroe.com` 網域，且其郵件位址爲 `user5@siroe.com`。
- 其使用提供者組織提供的清單中的一個或多個共用網域名稱。

  在圖 A–1 所示的範例中，共用組織 DEF 使用網域名稱 `siroe.com`。
- 其他共用組織可以共用此組織使用的網域名稱。

  在圖 A–1 所示的範例中，DEF 和 HIJ 組織都屬於 `siroe.com` 網域。
- 共用組織不具有唯一名稱空間。

建立提供者組織和服務提供者管理員

在此發行版本的 Delegated Administrator 中，您必須使用 Delegated Administrator 提供的自訂服務提供者範本 (`da.provider.skeleton.ldif`) 來建立您自己的提供者組織和 SPA。

備註 – 您也可以在執行 Delegated Administrator 配置程式時，在目錄中安裝提供者組織 (帶有從屬組織) 範例和 SPA 範例。您可以透過選擇配置程式中的 **[載入組織範例]** 來執行此作業。

但是，組織範本範例 (`da.sample.data.ldif`) 僅用做範例，而非建立自己的提供者組織的範本。如需有關此範例的詳細資訊，請參閱本附錄後面部分的第 147 頁的 「服務提供者組織資料範例」。

建立提供者組織和 SPA 後，SPA 即可登入 Delegated Administrator 主控台、建立和管理從屬組織以及將 SPA 角色指定給 SPA 組織中的其他使用者。但是，這些 SPA 只能管理同一提供者組織。

若要建立其他提供者組織和管理該組織的 SPA，您應再次使用自訂服務提供者範本。

本小節包含以下主題：

- 第 134 頁的 「範本建立的項目」顯示在目錄中安裝已編輯的範本時建立的組織之範例。
- 第 135 頁的 「建立提供者組織、從屬組織和 SPA 所需的資訊」定義範本中建立提供者組織、從屬共用組織和 SPA 所需的參數。
- 第 140 頁的 「建立提供者組織和服務提供者管理員的步驟」說明如何在目錄中編輯範本以及安裝資訊。
- 第 141 頁的 「自訂服務提供者範本」是範本清單。

範本建立的項目

在目錄中安裝已編輯的自訂服務提供者範本時，將建立以下項目：

- 提供者組織
- 被指定保留 SPA 使用者的從屬共用組織
- 從屬共用組織中一個被指定 SPA 角色的使用者
- 可以在其下建立完整組織的預留位置節點。這些完整組織將由此提供者組織的 SPA 管理。

圖 A–2 顯示了透過安裝範本建立的項目範例。其爲組織的目錄資訊樹狀結構 (DIT) 視圖。

圖 A–2 只是一個範例。您的組織名稱、SPA 使用者名稱和 DIT 結構應該特定於您自己的安裝。

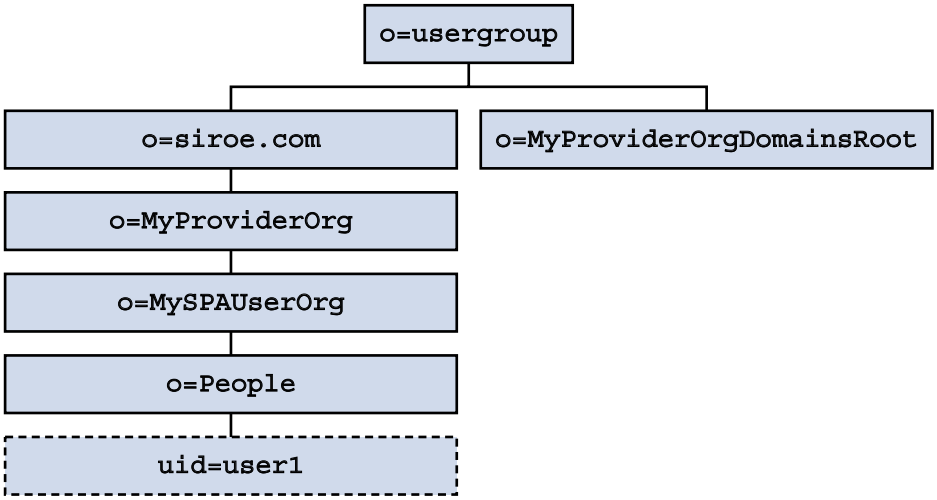

圖 A–2 自訂服務提供者範本：目錄資訊樹狀結構視圖

已安裝的自訂服務提供者範本範例中的節點

圖 A–2 所示範例中的節點如下：

- `o=usergroup` - 使用者/群組資料的根字尾。
- `o=siroe.com` - 提供者組織使用的郵件網域。
- `o=MyProviderOrg` - 提供者組織節點。
- `o=MySPAUserOrg` - 指定保留提供者組織使用者 (包含被指定 SPA 角色的使用者) 的從屬共用組織。
- `ou=people` - 包含使用者所需的標準 LDAP 組織單位。
- `uid=user1` - MySPAUserOrg 組織中被指定爲 SPA 的使用者的 uid。
- `o=MyProviderOrgDomainsRoot` - 用於保留從屬於 MyProviderOrg 提供者組織的完整組織的預留位置節點。

建立提供者組織、從屬組織和 SPA 所需的資訊

若要建立提供者組織、從屬組織和 SPA，您需要使用您的安裝的特定資訊替代自訂服務提供者範本中的參數。

若要瞭解這些參數，可以查看第 141 頁的 「自訂服務提供者範本」中所示的 `da.provider.skeleton.ldif` 清單。或開啓實際 ldif 檔案，該檔案位於以下目錄中：

da_base`/lib/config-templates`

如需與這些參數相關之屬性的定義，請參閱「*Sun Java System Communications Services Schema Reference*」中的「Chapter 5: Communications Services Delegated Administrator Classes and Attributes (Schema 2)」和「Chapter 3: Messaging Server and Calendar Server Attributes」。

定義提供者組織和從屬組織的參數

若要建立提供者組織和從屬組織，請編輯以下參數：

- *ugldapbasedn*

  目錄中使用者/群組資料的根字尾。

  範例：

  ```
  o=usergroup
  ```

  ```
  dc=red,dc=iplanet,dc=com
  ```

- *maildomain_dn*

  將在其下建立提供者組織的郵件網域的完整 DN。

  範例：

  ```
  o=siroe.com, o=usergroup
  ```

  ```
  o=sesta.com,o=SharedDomainsRoot,o=Business,dc=red, \
  dc=iplanet,dc=com
  ```

- *maildomain_dn_str*

  郵件網域 DN 中的所有逗號 (,) 都由底線 (_) 替代。

  例如，如果郵件網域 DN 爲

  ```
  o=siroe.com,o=SharedDomainsRoot,o=Business,dc=red, \
  dc=iplanet,dc=com
  ```

  郵件網域 DN 字串將爲

  ```
  o=siroe.com_o=SharedDomainsRoot_o=Business_dc=red_ \
  dc=iplanet_dc=com
  ```

- *providerorg*

  提供者組織的名稱。將爲提供者組織所在的目錄節點指定此名稱。

  此參數多次在 `da.provider.skeleton.ldif` 範本中使用。

  範例：

  ```
  sunProviderOrgDN: o=MyProviderOrg,o=siroe.com,o=usergroup
  ```

  ```
  o=MyProviderOrg
  ```

  ```
  sunBusinessOrgBase: o=MyProviderOrgdomainsroot, o=usergroup
  ```

- *servicepackage*

  可以指定給從屬於提供者組織的組織中使用者的服務套裝軟體的名稱。這是一個多值參數。

  在 `da.provider.skeleton.ldif` 檔案的 [提供者組織] 區段中，您將看到以下屬性：

```
sunIncludeServices: <servicepackage>
```

針對您要包含在提供者組織中的每個服務套裝軟體，增加一個 `sunIncludeServices` 屬性和 *servicepackage* 參數的實例。僅可將此處列出的這些服務套裝軟體指定給從屬組織中的使用者。

範例：

```
sunIncludeServices: gold
sunIncludeServices: platinum
sunIncludeServices: ruby
sunIncludeServices: silver
```

如果您未使用 `sunIncludeServices` 屬性 (如果您刪除包含 *servicepackage* 參數的行)，則可以指定目錄中的所有服務套裝軟體。

- *domain_name*

  可以指定給提供者組織中的從屬組織的網域名稱。這是一個多值參數。

  在 `da.provider.skeleton.ldif` 檔案的 [提供者組織] 區段中，您將看到以下屬性：

  ```
  sunAssignableDomains: <domain_name>
  ```

  `sunAssignableDomains` 屬性中的網域名稱是郵件網域組織的 `sunPreferredDomain` 和 `associatedDomain` 屬性中列出的名稱之子集 (一些或全部)。(郵件網域是其下建立此提供者組織的組織。)

  針對您要包含在提供者組織中的每個網域名稱，增加一個 `sunAssignableDomains` 屬性和 *domain_name* 參數的實例。僅可將此處列出的網域名稱指定給從屬組織。

  範例：

  ```
  sunAssignableDomains: siroe.com
  sunAssignableDomains: siroe.net
  sunAssignableDomains: varrius.com
  sunAssignableDomains: sesta.com
  sunAssignableDomains: sesta.net
  ```

- *provider_sub_org*

  SPA 使用者所在的共用組織的名稱。在目錄中安裝已編輯的 ldif 資訊時，會將該組織建立爲提供者組織的共用組織和從屬組織。該組織會被指定爲包含 SPA 使用者的組織。此提供者組織中被指定 SPA 角色的其他使用者必須在此從屬共用組織中。

  在 `da.provider.skeleton.ldif` 檔案的 [提供者組織] 區段中，您將看到以下屬性：

  ```
  sunProviderOrgDN:
  o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
  ```

  `sunProviderOrgDN` 屬性可識別爲提供者組織使用者，特別是 SPA 使用者指定的組織。

  範例：

  ```
  sunProviderOrgDN:
  o=MySPAUserOrg,o=MyProviderOrg,o=siroe.com,o=usergroup
  ```

- *preferredmailhost*

  提供者組織的從屬組織 (SPA 使用者所在的組織) 之喜好郵件主機的機器名稱。您必須使用完全合格的網域名稱 (FQDN)。

  在 da.provider.skeleton.ldif 檔案的 [共用從屬組織] 區段中，您將看到以下屬性：

  ```
  preferredMailHost: <preferredmailhost>
  ```

  範例：

  ```
  preferredMailHost: mail.siroe.com
  ```

- *available_domain_name*

  可以指定給特定從屬組織中使用者的網域名稱。這是一個多值參數。

  available_domain_name 的值是爲 sunAssignableDomains: <domain_name> 屬性和參數指定的值的適當子集。*domain_name* 套用於整個提供者組織，而 *available_domain_name* 套用於單一從屬組織。

  在 da.provider.skeleton.ldif 檔案的 [共用從屬組織] 區段中，您將看到以下屬性：

  ```
  sunAvailableDomainNames: <available_domain_name>
  ```

  針對您希望此從屬組織從提供者組織之 sunAssignableDomains 屬性中的網域名稱清單繼承的每個網域名稱，增加一個 sunAvailableDomains 屬性和 *available_domain_name* 參數的實例。僅可將此處列出的網域名稱指定給從屬組織。

  範例：

  ```
  sunAvailableDomainNames: siroe.com
  sunAvailableDomainNames: siroe.net
  sunAvailableDomainNames: varrius.com
  ```

- *available_services*

  可用於特定從屬組織的服務套裝軟體。這是一個多值參數。

  指定給從屬組織的服務套裝軟體是使用 sunIncludeServices 屬性指定給整個提供者組織的服務套裝軟體的子集。

  在 da.provider.skeleton.ldif 檔案的 [共用從屬組織] 區段中，您將看到以下屬性：

  ```
  sunAvailableServices: <available_services>
  ```

  available_services 參數的格式爲

  service package name: count

  其中，*count* 爲整數。如果缺少 count，則預設值爲無限制的數。

  針對您希望此從屬組織從提供者組織的 sunIncludeServices 屬性中可用的服務套裝軟體繼承之每個服務套裝軟體，增加一個 sunAvailableServices 屬性和 *available_services* 參數的實例。

  範例：

```
sunAvailableServices: gold:1500
sunAvailableServices: platinum:2000
sunAvailableServices: silver:5000
```

定義 SPA 的參數

若要建立 SPA，請編輯以下參數：

- *spa_uid*

  SPA 使用者的使用者 ID。

  範例：

  ```
  uid: user1
  ```

- *spa_password*

  SPA 使用者的密碼。

  範例：

  ```
  userPassword: x12P3&qrS
  ```

- *spa_firstname*

  SPA 使用者的名字。

  範例：

  ```
  givenname: John
  ```

- *spa_lastname*

  SPA 使用者的姓氏。

  範例：

  ```
  sn: Smith
  ```

- *spa_servicepackage*

  指定給 SPA 使用者的服務套裝軟體。如需有關服務套裝軟體的資訊，請參閱第 1 章中的第 30 頁的 「服務套裝軟體」。

  範例：

  ```
  inetCos: platinum
  ```

- *spa_mailaddress*

  SPA 使用者的郵件位址。郵件位址的網域部分必須是替代 *available_domain_name* 參數的網域值之一。亦即必須是可用於從屬組織 (SPA 使用者所在的組織) 中的網域。如需更多資訊，請參閱第 136 頁的 「定義提供者組織和從屬組織的參數」。

  範例：

  ```
  mail: user1@siroe.com
  ```

如需有關如何在目錄中編輯自訂服務提供者範本和安裝資訊的說明，請參閱第 140 頁的 「建立提供者組織和服務提供者管理員的步驟」。

建立提供者組織和服務提供者管理員的步驟

您可以使用 ldif 檔案 `da.provider.skeleton.ldif` 執行以下程序。

▼ 建立提供者組織和服務提供者管理員

步驟 1. **在目錄中建立郵件網域**。

如果您尚未建立郵件網域，請在目錄中執行此作業。提供者組織及其從屬共用組織將使用此郵件網域。

2. **複製並重新命名 `da.provider.skeleton.ldif` 檔案**。

安裝 Delegated Administrator 時，`da.provider.skeleton.ldif` 檔案會安裝在以下目錄中：

da_base `/lib/config-templates`

3. **在 `da.provider.skeleton.ldif` 檔案副本中編輯以下參數。使用對於您的安裝正確的值替代這些參數**。

如需參數的定義，請參閱第 135 頁的 「建立提供者組織、從屬組織和 SPA 所需的資訊」。

某些參數在 ldif 檔案中使用多次。您必須搜尋並替代每個參數的所有實例。

一些參數代表多值屬性的值。您可以複製和編輯這些參數及其關聯屬性名稱，以允許 ldif 檔案中存在這些屬性的多個實例。以下註明了多值參數。

- `<ugldapbasedn>`
- `<maildomain_dn>`
- `<maildomain_dn_str>`
- `<providerorg>`
- `<servicepackage>` (多值)
- `<domain_name>` (多值)
- `<provider_sub_org>`
- `<preferredmailhost>`
- `<available_domain_name>` (多值)
- `<available_services>` (多值)
- `<spa_uid>`
- `<spa_password>`
- `<spa_firstname>`
- `<spa_lastname>`
- `<spa_servicepackage>`

- <spa_mailaddress>

  如需與這些參數相關之屬性的定義，請參閱「*Sun Java System Communications Services Schema Reference*」中的「Chapter 5: Communications Services Delegated Administrator Classes and Attributes (Schema 2)」和「Chapter 3: Messaging Server and Calendar Server Attributes」。

4. **使用 LDAP 目錄工具 `ldapmodify` 在目錄中安裝提供者組織和 SPA。**

   例如，您可以執行以下指令：

```
ldapmodify -D <directory manager> -w <password> \
-f <da.provider.finished.ldif>
```

   其中，

   <directory manager> 是 Directory Server 管理員的名稱。

   <password> 是 Directory Service 管理員的密碼。

   <da.provider.finished.ldif> 是要做爲新的提供者組織和 SPA 安裝在目錄中的已編輯 ldif 檔案的名稱。

自訂服務提供者範本

範本 (da.provider.skeleton.ldif) 包含您必須修改以建立新的提供者組織和 SPA 的參數。

下面的清單顯示 ldif 檔案中具有參數的區段。該清單未包含整個檔案。此處未包含支援 Access Manager 所需的項目和 ACI。

您應僅修改 ldif 檔案中的參數。請勿修改與 Access Manager 相關的檔案區段。

da.provider.skeleton.ldif 檔案 (相關區段)

```
#
# The following parameterized values must be replaced.
#
# <ugldapbasedn>          :: Root suffix for user/group data
# <maildomain_dn>         :: Complete dn of the mail domain underneath
#                            which the provider organization will be
#                            created.
# <maildomain_dn_str>     :: The maildomain dn with all ',' replaced
#                                      by '_'. E.g.
#                            dn --\> o=siroe.com,o=SharedDomainsRoot,
#                            o=Business,dc=red,dc=iplanet,dc=com
#                            dn_str --> o=siroe.com_o=SharedDomainsRoot_
#                            o=Business_dc=red_dc=iplanet_dc=com
# <providerorg>            : Organization value for provider node.
# <servicepackage>        :: One for each service package to include.
```

```
#                              All service packages in the system
#                              may be assigned by leaving this value empty.
# <domain_name>             :: One for each DNS name which may be assigned
#                              to a subordinate organization.
#                              These names form a proper subset (some or
#                              all) of the names listed in the <maildomain>
#                              organization's sunpreferreddomain
#                              and associateddomain attributes.
# <provider_sub_org>        :: Organization value for the shared subordinate
#                              organization in which the Provider
#                              Administrator resides.
# <preferredmailhost>       :: Name of the preferred mail host for the
#                              provider's subordinate organization.
# <available_domain_name>   :: one for each DNS name that an organization
#                              allows an organization admin to use when
#                              creating a user's mail address.  This is
#                              a proper subset of the values given for
#                              <domain_name> (sunAssignableDomains attribute).
# <available_services>      :: One for each service packags available to an
#                              organization (sunAvailableServices attribute).
#                              These service packages form a proper subset
#                              of the ones assigned to a provider organization
#                              - <servicepackage> (sunIncludeServices
#                              attribute).  Form is
#                              <service package name>:<count>
#                              where count is an integer.  If count is absent
#                              then default is unlimited.
# <spa_uid>                 :: The uid for the service provider administrator.
# <spa_password>            :: The password for the service provider
#                              administrator.
# <spa_firstname>           :: First name of the service provider
#                              administrator.
# <spa_lastname>            :: Last name of the service provider
#                              administrator.
# <spa_servicepackage>      :: Service package assigned to the service
#                              provider administrator.
# <spa_mailaddress>         :: The spa's mail address. The domain part of the
#                              mail address must be one of the values used for
#                              <available_domain_name>.
#


#
# Provider Organization
#
dn: o=<providerorg>,<maildomain_dn>
changetype: add
o: <providerorg>
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunmanagedorganization
objectClass: organization
objectClass: sunManagedProvider
sunAllowBusinessOrgType: full
sunAllowBusinessOrgType: shared
```

```
sunBusinessOrgBase: o=<providerorg>domainsroot,<ugldapbasedn>
sunIncludeServices: <servicepackage>
sunAssignableDomains: <domain_name>
sunAllowMultipleDomains: true
sunAllowOutsideAdmins: false
sunProviderOrgDN: o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# Full Organizations node
#
dn: o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
o: <providerorg>DomainsRoot
objectClass: top
objectClass: organization
objectClass: sunmanagedorganization
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# Provider Admin Role shared organizations
#
dn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
objectClass: top
iplanet-am-role-description: Provider Admin

#
# Provider Admin Role full organizations
#
dn: cn=Provider Admin Role,o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
objectClass: top
iplanet-am-role-description: Provider Admin
```

```
#
# Shared Subordinate Organization. Includes 1 user who is
# the Provider Administrator.
#
dn: o=<provider_sub_org>,=<providerorg>,<maildomain_dn>
changetype: add
preferredMailHost: <preferredmailhost>
sunNameSpaceUniqueAttrs: uid
o: <provider_sub_org>
objectClass: inetdomainauthinfo
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunnamespace
objectClass: sunmanagedorganization
objectClass: organization
objectClass: sunDelegatedOrganization
objectClass: sunMailOrganization
sunAvailableDomainNames: <available_domain_name>
sunAvailableServices: <available_services>
sunOrgType: shared
sunMaxUsers: -1
sunNumUsers: 1
sunMaxGroups: -1
sunNumGroups: 0
sunEnableGAB: true
sunAllowMultipleServices: true
inetDomainStatus: active
sunRegisteredServiceName: GroupMailService
sunRegisteredServiceName: DomainMailService
sunRegisteredServiceName: UserMailService
sunRegisteredServiceName: iPlanetAMAuthService
sunRegisteredServiceName: UserCalendarService
sunRegisteredServiceName: iPlanetAMAuthLDAPService
sunRegisteredServiceName: DomainCalendarService
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

dn: ou=People,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: People
objectClass: iplanet-am-managed-people-container
objectClass: organizationalUnit
objectClass: top

dn: ou=Groups,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: Groups
objectClass: iplanet-am-managed-group-container
objectClass: organizationalUnit
objectClass: top
# .
# .
```

```
# [Entries and ACIs required by Access Manager]
# .
# .

#
# User - provider administrator
#
dn: uid=<spa_uid>,ou=People,o=<provider_sub_org>,o=<providerorg>, \
        <maildomain_dn>
changetype: add
sn: <spa_lastname>
givenname: <spa_firstname>
cn:  <spa_firstname> <spa_lastname>
uid: <spa_uid>
iplanet-am-modifiable-by: cn=Top-level Admin Role,<ugldapbasedn>
objectClass: inetAdmin
objectClass: top
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: iPlanetPreferences
objectClass: person
objectClass: organizationalPerson
objectClass: inetuser
objectClass: inetOrgPerson
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: inetSubscriber
objectClass: userPresenceProfile
objectClass: icsCalendarUser
mailhost: <preferredmailhost>
mail: <spa_mailaddress>
maildeliveryoption: mailbox
mailuserstatus: active
inetCos: <spa_servicepackage>
inetUserStatus: Active
nsroledn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
userPassword: <spa_password>
```

建立共用和完整從屬組織

建立提供者組織和 SPA 之後，SPA 即可建立和管理從屬於該提供者組織的共用組織和完整組織。SPA 使用 Delegated Administrator 主控台完成這些作業。

以下作業概述建立共用組織或完整組織的關鍵步驟。此作業未說明如何輸入使用 [建立新組織] 精靈建立組織時顯示的所有資訊。如需 [建立新組織] 精靈的詳細說明，請參閱 Delegated Administrator 主控台線上說明。

▼ 建立共用或完整從屬組織

步驟 1. **啓動 Delegated Administrator 主控台**。

請至以下 URL：

`http://`*host*`:` *port*`/da/DA/Login`

其中，

host 是 Web 容器主機電腦

port 是 Web 容器連接埠

例如：

`http://siroe.com:8080/da/DA/Login`

螢幕上將顯示 Delegated Administrator 主控台登入視窗。

2. **使用 SPA 登入 ID 和密碼登入 Delegated Administrator 主控台**。

前面的小節第 133 頁的 「建立提供者組織和服務提供者管理員」說明了如何建立 SPA。

螢幕上將顯示 [服務提供者管理員] 頁面。依預設，選取 [組織] 標籤。此頁面顯示從屬於 SPA 的提供者組織的組織。

3. **按一下 [新建組織]**。

螢幕上將顯示 [建立新組織] 精靈。如需有關在 [建立新組織] 精靈中輸入和選取資訊的詳細資訊，請參閱 Delegated Administrator 主控台線上說明。

4. **在 [組織資訊] 面板中輸入資訊，然後按 [下一步]**。

螢幕上將顯示 [聯絡人資訊] 面板。

5. **在 [聯絡人資訊] 面板中輸入資訊，然後按 [下一步]**。

螢幕上將顯示 [帳號資訊] 面板。

6. **選擇建立共用組織還是完整組織**。

在 [帳號資訊] 面板中，您可以確定新組織是共用組織還是完整組織。

共用組織使用與其他組織共用的現有網域。

完整組織具有其自己的唯一網域。

- 若要建立共用組織，請按一下 **[從可用網域中選取]** 單選按鈕。

  從下拉式清單中選擇網域。

備註 – 建立共用組織時，會從現有父系網域繼承行事曆服務詳細資訊。因此，您不必爲新組織輸入行事曆服務資訊。[行事曆服務詳細資訊] 面板將不會顯示在 [建立新組織] 精靈中。而且建立共用組織之後，[行事曆服務詳細資訊] 不會顯示在組織的 [特性] 頁面中。

- 若要建立完整組織，請按一下 **[新建網域]** 單選按鈕。

  在文字方塊中，輸入新的郵件網域名稱。例如：`siroe.com`。

  如果願意，您可以在 **[新網域的別名]** 文字方塊中爲新網域輸入別名。

7. **在 [建立新組織] 精靈的剩餘面板中輸入資訊。**

   如需有關這些面板的詳細資訊，請參閱 Delegated Administrator 主控台線上說明。

服務提供者組織資料範例

執行 Delegated Administrator 配置程式 `config-commda` 時，您可以選擇在目錄中安裝組織資料 (在 ldif 檔案中定義) 範例。(執行配置程式時，選取 **[服務套裝軟體和組織範例]** 面板中的 **[載入組織範例]**。)配置程式將 `da.sample.data.ldif` 檔案增加至 LDAP 目錄樹狀結構中。

此 ldif 檔案僅用做範例，而非建立您自己的提供者組織的範本。若要建立新的提供者組織，請參閱第 135 頁的 「建立提供者組織、從屬組織和 SPA 所需的資訊」。

資料範例提供的組織

圖 A–1 顯示了 ldif 檔案範例提供的組織結構的邏輯視圖。(圖 A–1 增加了檔案中不存在的共用組織 HIJ。)

ldif 檔案範例在根字尾節點下包含以下組織：

- VIS 提供者組織。VIS 提供者組織的 SPA 管理以下組織：
  - 完整組織 SESTA。SESTA 組織具有其自己的網域 `sesta.com`。
  - 共用組織 DEF。DEF 組織使用共用網域 `siroe.com`。
- ESG 提供者組織。沒有爲此提供者組織定義任何從屬組織。

ldif 檔案爲這些組織定義以下管理員角色：

- VIS 提供者組織 (`user2@abc.com`) 的 SPA
- ESG 提供者組織 (`user2_def`) 的 SPA
- SESTA 組織 (`user1@abc.com`) 的 OA

- DEF 組織 (`user1_def`) 的 OA

邏輯階層和目錄資訊樹狀結構

在三階式目錄階層中，目錄資訊樹狀結構 (DIT) 與圖 A–1 中所示的邏輯視圖不完全一樣。組織在稍微不同的階層的 DIT 中實作。

例如，在 DIT 中，完整網域必須直接在根字尾之下。因此，網域節點會增加至根字尾下，以儲存共用網域 (由共用組織使用) 和完整組織 (具有其自己的網域) 的 LDAP 資訊。

組織資料範例：目錄資訊樹狀結構視圖

圖 A–3 顯示了組織資料範例的目錄資訊樹狀結構 (DIT) 視圖。

如圖 A–1 中所示的邏輯視圖一樣，圖 A–3 中所示的範例包含以下組織：

- VIS 和 ESG (提供者組織)
- DEF，從屬於 VIS 提供者組織的共用組織
- SESTA，從屬於 VIS 提供者組織的完整組織

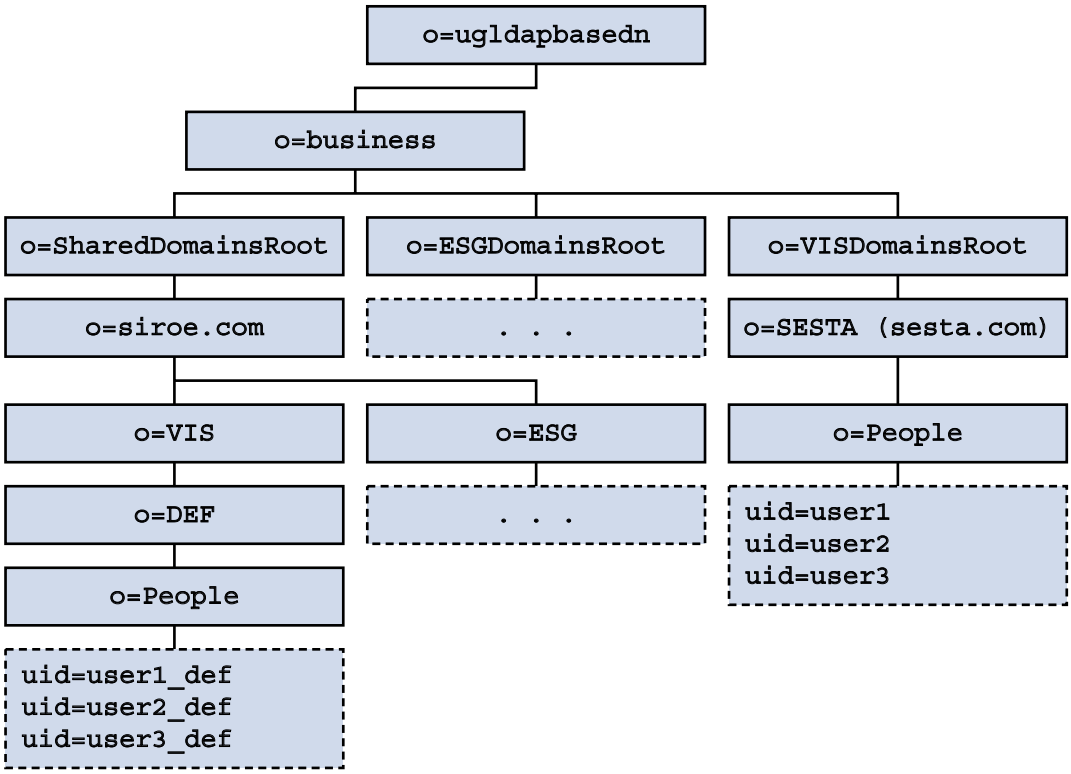

圖 A–3 組織資料範例：目錄資訊樹狀結構視圖

目錄資訊樹狀結構範例中的節點

組織檔案範例 (`da.sample.data.ldif`) 中的節點如下：

- *ugldapbasedn* - 此參數代表根字尾。
- `o=business` - 包含目錄中所有企業的節點。
- `o=SharedDomainsRoot` - 包含共用組織使用的網域所需的節點。

  在此目錄資訊樹狀結構中，從屬於不同服務提供者組織的共用組織可以使用同一共用網域。這是因爲，兩個提供者組織在 `SharedDomainsRoot` 節點下都有節點。
- `o=ESGDomainsRoot` 和 `o=VISDomainsRoot` - 這兩個節點包含從屬於 ESG 和 VIS 提供者組織的所有完整組織。

  管理完整組織的每個提供者組織在此層級 (在根字尾下) 都必須具有節點。

  `ESGDomainsRoot` 或 `VISDomainsRoot` 下可以存在多個完整組織，每個都有其自己的網域。
- `o=siroe.com` - 共用網域。其由共用組織 DEF 使用。

- o=VIS 和 o=ESG - 這兩個提供者組織節點包含從屬於 VIS 和 ESG 提供者組織的所有共用組織。

  例如，共用組織 DEF 從屬於 VIS 提供者組織。
- o=SESTA - 完整組織。其具有自己的網域 sesta.com。
- o=DEF - 共用組織。其使用網域 siroe.com。
- ou=people - 包含使用者所需的標準 LDAP 組織單位。

目錄資訊樹狀結構範例中的使用者 *DN*

圖 A–3 所示的組織檔案範例中的某些使用者 DN 如下：

- 對於屬於 DEF 組織的名爲 user1_def 的使用者：

  dn: uid=user1_def,ou=People,o=DEF,o=VIS,o=siroe.com,
  o=SharedDomainsRoot,o=Business,*ugldapbasedn*
- 對於屬於 SESTA 組織的名爲 user1 的使用者：

  dn: uid=user1,ou=People,o=SESTA,o=VISDomainsRoot,
  o=Business,*ugldapbasedn*

附錄 B

屬性值和行事曆時區

屬性值

表 B–1 中列出的屬性可與以下指令的 `-P` 選項配合使用：第 96 頁的 「commadmin domain create」和第 100 頁的 「commadmin domain modify」。這些屬性爲位元導向屬性，或多值屬性。

表 B–1 用於 `-P` 選項的屬性

屬性	值	說明
`createLowerCase`	yes/no	指定是否要爲新使用者建立小寫行事曆。同時，指定在查詢行事曆時是否查詢小寫行事曆。
`filterPrivateEvents`	yes/no	指定在查詢伺服器時是否篩選私密或機密事件
`fbIncludeDefCal`	yes/no	指定使用者的預設行事曆是否包含在使用者的 `freebusy-calendar-list` 中。
`subIncludeDefCal`	yes/no	指定是否要將使用者的預設行事曆包含在使用者的 `subscribed-calendar-list` 中
`resourceDefaultAcl`	yes/no	指定是否對資源行事曆使用預設 ACL。
`calmasterCred`	字串	指定做爲 Calendar Server 管理員的使用者憑證。
`calmasterUid`	字串	`service.admin.calmaster.userid`
`calmasterAccessOverride`	yes/no	指定 Calendar Server 管理員是否可以置換存取控制。

表 B–1 用於 -P 選項的屬性　　(續)

屬性	值	說明
setPublicRead	yes/no	將預設使用者行事曆設定爲公開讀取或私密寫入。如果選取 no，則會將使用者行事曆設定爲私密讀取或私密寫入。
uiBaseUrl	字串	BaseServerAddress，例如 https://proxyserver/
uiConfigFile	字串	使用者介面的配置檔案。
uiProxyUrl	字串	附加在 HTML 使用者介面之 JavaScript 檔案中的代理伺服器位址。例如，https://web_portal.iplanet.com/
domainAccess	字串	網域的存取控制字串。用於跨網域搜尋。
uiAllowAnyone	yes/no	指定是否允許 HTML 使用者介面顯示並使用「Everybody」ACL。
allowProxyLogin	yes/no	指定是否允許代理伺服器登入

表 B–2 中列出的屬性可與以下指令的 -R 選項配合使用：第 96 頁的 「commadmin domain create」和第 100 頁的 「commadmin domain modify」。屬性具有位元導向值。

如需有關 WCAP 和 WCAP set-userprefs 指令的資訊，請參閱「*Sun Java System Calendar Server Programmer's Manual*」。

表 B–2 用於 -R 選項的屬性

屬性	值	說明
allowUserDoubleBook	bit 8	允許在同一時段對此行事曆進行多次排程。
allowResourceDoubleBook	bit 9	允許在同一時段對此資源行事曆進行多次排程。
allowModifyUserPreferences	bit 4	允許 Calendar Server 管理員應從 WCAP 爲使用者取得 get/set userprefs。
allowModifyPassword	bit 5	允許使用者經由此伺服器變更其密碼。
allowCalendarCreation	bit 0	允許建立行事曆。
allowCalendarDeletion	bit 1	允許刪除行事曆。
allowPublicWritableCalendars	bit 2	允許使用者擁有公開可寫入行事曆。
allowSetCn	bit 10	允許 set-userprefs.wcap 修改 cn 使用者喜好設定。

表 B–2 用於 -R 選項的屬性　　(續)

屬性	值	說明
allowSetGivenName	bit 11	允許 set_userprefs.wcap 修改 givenname 使用者喜好設定。
allowSetGivenMail	bit 12	允許 set_userprefs.wcap 修改 mail 使用者喜好設定。
allowSetPrefLang	bit 13	允許 set_userprefs.wcap 修改 preferredlanguage 使用者喜好設定。
allowSetSn	bit 14	允許 set-userprefs.wcap 修改 sn 使用者喜好設定。

行事曆時區字串

以下時區字串可以與第 96 頁的 「commadmin domain create」、第 100 頁的 「commadmin domain modify」、第 113 頁的 「commadmin resource create」、第 117 頁的 「commadmin resource modify」、第 120 頁的 「commadmin user create」以及第 124 頁的 「commadmin user modify」指令的 -T 時區選項配合使用：

還可以增加新的時區並將其設定爲預設時區。如需詳細資訊，請參閱第 85 頁的 「增加新的行事曆時區」。

- 非洲/開羅
- 非洲/卡薩布蘭加
- 非洲/約翰尼斯堡
- 非洲/拉哥斯
- 非洲/的黎波里
- 非洲/文胡克
- 美洲/艾達克
- 美洲/安克治
- 美洲/布宜諾賽利斯
- 美洲/卡拉卡斯
- 美洲/芝加哥
- 美洲/哥斯大黎加
- 美洲/古雅巴
- 美洲/丹佛
- 美洲/哥特哈布
- 美洲/大特克
- 美洲/哈利法克斯
- 美洲/哈瓦那
- 美洲/印第安納波利
- 美洲/洛杉磯

- 美洲/密啓倫
- 美洲/紐約
- 美洲/費尼克斯
- 美洲/太子港
- 美洲/聖地牙哥
- 美洲/聖保羅
- 美洲/聖約翰斯
- 亞洲/阿拉木圖
- 亞洲/安曼
- 亞洲/阿納底
- 亞洲/阿克圖
- 亞洲/阿克托貝
- 亞洲/巴庫
- 亞洲/曼谷
- 亞洲/貝魯特
- 亞洲/比斯凱克
- 亞洲/加爾各答
- 亞洲/達卡
- 亞洲/伊爾庫次克
- 亞洲/耶路撒冷
- 亞洲/喀布爾
- 亞洲/勘察加
- 亞洲/喀拉蚩
- 亞洲/加德滿都
- 亞洲/克拉斯諾雅
- 亞洲/馬加丹
- 亞洲/新西伯利亞
- 亞洲/仰光
- 亞洲/利雅德
- 亞洲/上海
- 亞洲/東京
- 亞洲/烏蘭巴托
- 亞洲/海參崴
- 亞洲/雅庫次克
- 亞洲/凱薩琳堡
- 亞洲/葉勒凡
- 大西洋/阿速爾
- 大西洋/維德角
- 大西洋/南喬治
- 大西洋/史坦萊
- 澳大利亞/阿得雷德
- 澳大利亞/布利斯班
- 澳大利亞/達爾溫
- 澳大利亞/荷巴特
- 澳大利亞/羅豪
- 澳大利亞/雪梨
- 歐洲/布加勒斯
- 歐洲/伊斯坦堡

- 歐洲/倫敦
- 歐洲/明斯克
- 歐洲/莫斯科
- 歐洲/巴黎
- 歐洲/里加
- 歐洲/沙馬拉
- 歐洲/新佛洛普
- 歐洲/華沙
- 太平洋/亞庇
- 太平洋/奧克蘭
- 太平洋/查坦
- 太平洋/伊斯特
- 太平洋/斐濟
- 太平洋/甘比爾
- 太平洋/瓜達卡納
- 太平洋/檀香山
- 太平洋/基里蒂馬蒂
- 太平洋/馬克沙斯
- 太平洋/諾福克
- 太平洋/諾美亞
- 太平洋/皮特康
- 太平洋/拉洛東加
- 太平洋/東加塔普

附錄 C

對 Delegated Administrator 進行除錯

可以透過檢查由 Delegated Administrator 元件、部署 Delegated Administrator 的 Web 容器、Directory Server 和 Access Manager 產生的記錄檔來取得 Delegated Administrator 的記錄資訊。

本附錄包含以下主題：

對指令行公用程式進行除錯

若要對 Delegated Administrator 公用程式 (`commadmin`) 進行除錯，可以透過將 `-v` 選項和 `commadmin` 指令配合使用，在用戶端顯示除錯訊息。

Delegated Administrator 主控台記錄

Delegated Administrator 主控台會建立執行階段記錄檔：

- 預設記錄檔名稱：`da.log`
- 預設位置：`/opt/SUNWcomm/log`

可以透過編輯記錄特性檔案來指定自己的記錄檔：

- 記錄特性檔案名稱：`logger.properties`

- 預設位置：

  ```
  /var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/ \
  comm/da/resources
  ```

可以在 logger.properties 檔案中變更以下特性：

- `da.logging.enable=yes` 或 `no`

  其中，`yes` 將啓用記錄功能，而 `no` 將停用記錄功能。

  依預設，記錄功能處於停用狀態。若要啓用記錄功能，必須將此值設定爲 `yes`。

- `da.log.file=`*full pathname*

  指定記錄敘述要寫入的目錄和檔案。此特性會將 `da.log` 變更爲您指定的檔案名稱和位置。

Delegated Administrator 伺服器記錄

可以建立 Delegated Administrator 伺服器記錄，該記錄包含由安裝在 Web 容器中的 Delegated Administrator Servlet 產生的除錯敘述。

若要執行此作業，可以啓用 Debug Servlet 來記錄 Delegated Administrator Servlet 執行中的除錯訊息。可以透過至以下 URL 路徑經由瀏覽器開啓 Debug Servlet：

`http://`*machine name*`:`*port*`/commcli/debug?op=set&state=all&package=all&filename=`*full path*

其中，

- *machine name* 是執行 Delegated Administrator 伺服器的機器名稱。
- *full path* 是訊息要寫入的記錄之完整目錄路徑和名稱。

例如：

```
http://abc.red.iplanet.com:8008/commcli/debug?op= \
set&state=all&package=all&filename=/tmp/debug.log
```

前面的 URL 會將 Debug Servlet 訊息記錄至以下路徑和檔案：

```
/tmp/debug.log
```

在每次重新啓動 Web 容器時，均必須開啓 Debug Servlet。

Web 容器伺服器記錄

還可以透過檢查 Web 容器所產生的伺服器記錄，進一步對 Delegated Administrator 進行除錯。

Web Server

Web Server 可維護位於以下路徑的存取記錄和錯誤記錄：

/web_server_base/`https-`*machine name*/`logs`

其中，

- *web_server_base* 是 Web Server 軟體的安裝路徑。
- *machine name* 是執行 Web Server 的機器名稱。

Application Server 7.*x*

Application Server 7.*x* 可維護位於以下路徑的存取記錄和錯誤記錄：

/application_server7_base/`domains/domain1/server1/logs`

其中，

- *application_server7_base* 是 Application Server 7.*x* 軟體的安裝路徑。

Application Server 8.*x*

Application Server 8.*x* 可維護位於以下路徑的存取記錄和錯誤記錄。

伺服器記錄：

/application_server8_base/`domains/domain1/logs`

存取記錄：

/application_server8_base/`domains/domain1/logs/access/server_access_log`

其中，

- *application_server8_base* 是 Application Server 8.*x* 軟體的安裝路徑。

Directory Server 和 Access Manager 記錄

還可以透過檢查由 Directory Server 和 Access Manager 產生的記錄，進一步對 Delegated Administrator 進行除錯。

Directory Server

Directory Server 可維護位於以下路徑的存取記錄和錯誤記錄：

`/var/opt/mps/serverroot/slapd-`*hostname* `/logs`

其中，

- *hostname* 是執行 Directory Server 的機器名稱。

Access Manager

Access Manager 可維護位於以下路徑中的記錄檔：

`/var/opt/SUNWam/debug`

前面的路徑包含 `amProfile` 和 `amAuth` 記錄。

`/var/opt/SUNWam/logs`

前面的路徑包含 `amAdmin.access` 和 `amAdmin.error` 記錄。

附錄 D

Delegated Administrator 效能調校

以下主題說明如何調校 Delegated Administrator 以及相關軟體，以提昇 Delegated Administrator 效能：

除在此附錄中說明的以下使用準則之外，還可以透過合併和減少目錄中的預設 ACI 數來提昇 Directory Server 效能。如需有關資訊，請參閱附錄 E。

加速顯示使用者、群組和組織

如果組織包含多個使用者，Delegated Administrator 主控台可能需要耗用一段時間來顯示 [使用者] 清單頁面。如果在頁面仍在載入現有使用者時嘗試建立或編輯該使用者，將發生錯誤。在頁面完全載入之前，請勿按任何按鈕或連結。

同樣，如果目錄包含多個組織或群組，Delegated Administrator 主控台可能也需要耗用一段時間來開啓 [組織] 頁面或 [群組] 頁面。

如果載入這些頁面耗用時間過長，可以將萬用字元搜尋特性設定爲足夠小的值，以快速載入頁面。

這些特性爲：

jdapi-wildusersearchmaxresults	用於使用者的搜尋特性。
jdapi-groupsmaxsearchresults	用於群組的搜尋特性。
jdapi-wildorgsearchmaxresults	用於組織的搜尋特性。

萬用字元搜尋特性限制如下：

`-1`	傳回所有結果。(顯示所有使用者、群組或組織。) `-1` 爲預設值。

`0` 不搜尋。(不顯示使用者、群組或組織。)

n（>0） 傳回 *n* (指定的結果數) 個。

▼ 更快速顯示 [使用者] 頁面

步驟 **1. 開啓 `resource.properties` 檔案。**

`resource.properties` 檔案位於以下目錄中：

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

2. 將 `jdapi-wildusersearchmaxresults` 值設定為較小的值。例如：

```
jdapi-wildusersearchmaxresults=50
```

或者，可以將此值設定爲 `0`，不顯示使用者。在 Delegated Administrator 主控台中，使用 **[搜尋]** 下拉式清單搜尋指定的使用者。

▼ 更快速顯示 [群組] 頁面

步驟 **1. 開啓 `resource.properties` 檔案。**

`resource.properties` 檔案位於以下目錄中：

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

2. 將 `jdapi-groupsmaxsearchresults` 值設定為較小的值。例如：

```
jdapi-groupsmaxsearchresults=50
```

或者，可以將此值設定爲 `0`，不顯示群組。在 Delegated Administrator 主控台中，使用 **[搜尋]** 下拉式清單搜尋指定的群組。

▼ 更快速顯示 [組織] 頁面

步驟 **1. 開啓 `resource.properties` 檔案。**

`resource.properties` 檔案位於以下目錄中：

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

2. **將 `jdapi-wildorgsearchmaxresults` 值設定為較小的值。例如：**

   ```
   jdapi-wildusersearchmaxresults=10
   ```

   或者，可以將此值設定爲 `0`，不顯示組織。在 Delegated Administrator 主控台中，使用 **[搜尋]** 下拉式清單搜尋指定的組織。

增加 JVM 堆疊大小

若要提昇 Delegated Administrator 常用功能 (如顯示頁面和執行搜尋) 的效能，可以增加部署 Delegated Administrator 之 Web 容器所使用的 Java Virtual Machine (JVM) 堆疊大小。如果 Web 容器的 JVM 堆疊過小，可能會影響效能。

可透過以下 JVM 選項設定 JVM 堆疊大小：

`-Xmx<`*n*`>m`

其中，<*n*> 爲堆疊大小 (以百萬位元組表示)。

通常，<*n*> 設定爲 `256m`。

以下作業概述如何爲 Web Server 和 Application Server 設定更高的 JVM 堆疊大小。

▼ 增加 Web Server JVM 堆疊大小

步驟

1. **登入 Web Server Administration Server。**
2. **在 [Java] 標籤下，選取 [JVM 選項]。**
3. **編輯 `-Xmx256m` 選項。**
   此選項可設定 JVM 堆疊大小。
4. **將 `-Xmx256m` 選項設定為較高的值，例如 `Xmx1024m`。**
5. **儲存新設定。**

更多資訊 Web Server 文件

請參閱「Sun Java System Web Server Administration Guide」以及「Web Server Performance Tuning, Sizing, and Scaling Guide」，以取得有關使用 Web Server Administration Server 和設定 JVM 選項的更多資訊。

▼ 增加 Application Server JVM 堆疊大小

步驟

1. **登入 Application Server Administration Server**。
2. **瀏覽至 JVM 選項**。
3. **編輯 `-Xmx256m` 選項**。
   此選項可設定 JVM 堆疊大小。
4. **將 `-Xmx256m` 選項設定為較高的值，例如 `Xmx1024m`**。
5. **儲存新設定**。

更多資訊 Application Server 文件

如需有關使用 Application Server Administration Server 和設定 JVM 選項的更多資訊，請至「Sun Java System Application Server Documentation Center」，並選取「JVM Advanced Settings」。或者，請參閱「Sun Java System Application Server Enterprise Edition 8.1 2005Q4 Performance Tuning Guide」中的「Tuning the Java Runtime System」

增加 Directory Server 索引建立臨界值

若要提昇 Delegated Administrator 功能 (例如搜尋和顯示使用者) 的效能，可以增加 Directory Server 用於搜尋目錄的索引建立之臨界值。

Directory Server 搜尋大量 LDAP 物件時，如果將臨界值設定爲較小的值，則搜尋完成之前，索引建立可能會發生空間不足的問題。執行剩餘搜尋項目時將不再建立索引，因爲建立索引會使搜尋作業速度減慢。

注意 – 僅當您是有經驗的 Directory Server 管理員時執行此作業。

若要將索引臨界值設定爲較高的值，請變更 `dse.ldif` 檔案中 `nssldap-allidsthreshold` 選項的值

可將此選項設定爲如下值：

```
nssldap-allidsthreshold: 4000
```

將 `nssldap-allidsthreshold` 設定爲較高的值。例如：

```
nssldap-allidsthreshold: 200000
```

如需有關所有 ID 臨界值的更多資訊，請參閱「Sun Java System Directory Server Administration Guide」「Indexing Directory Data」中的「Managing Indexes」。如需 `nssldap-allidsthreshold` 選項定義，請參閱「Sun Java System Directory Server Administration Reference」中「Server Configuration Reference」中的「Database Configuration Attributes」。

附錄 E

合併 ACI 以提昇 Directory Server 效能

本附錄說明以下主題：

簡介

將 Messaging Server 與 Access Manager 同時安裝，且使用 LDAP Schema 2 目錄時，最初將在該目錄中安裝大量存取控制指令 (ACI)。Messaging Server 並不需要或使用許多預設 ACI。

由於在執行階段需要檢查這些ACI，Directory Server 的效能會受到影響，繼而影響 Messaging Server 查詢以及其他目錄作業的效能。

可以透過合併和減少目錄中的預設 ACI 數來提昇 Directory Server 的效能。合併 ACI 還可以使其更易於管理。

減少 ACI 的方法爲：

- 合併、最佳化以及簡化備援 ACI
- 修改 ACI 以使用更簡單、更高效的語法
- 將 ACI 與其他 ACI 合併 (在根字尾處)
- 刪除未使用的 ACI
- 對於包含多個組織的目錄，允許在個別組織節點上移除組織 ACI。

本附錄首先說明如何使用 ldif 檔案 (`replacment.acis.ldif`) 在根字尾處合併 ACI 以及從目錄中移除未使用的 ACI。如需詳細資訊，請參閱以下第 168 頁的 「合併和移除 ACI」。

然後，附錄會分析每個 ACI，並推薦處理每個 ACI 的方法： 移除 ACI、修改 ACI 使其更高效或重寫 ACI。

請注意，這些推薦方法存在以下限制：

- 一般使用者無法存取 Directory 主控台
- 一般使用者無法存取 Access Manager 主控台。

必須根據這些限制以及您的安裝需求自行決定是否可以使用 ldif 檔案合併和移除 ACI，或者是否需要保留目前存在於目錄中的某些ACI。

如需更多資訊，請參閱本附錄後面部分的第 172 頁的 「分析現有 ACI」。

然後，本附錄將說明由 `replacement.acis.ldif` 檔案合併的 ACI。本附錄列出合併之前的現有 ACI 以及合併之後已修改的 ACI。如需更多資訊，請參閱本附錄後面部分的第 188 頁的 「分析如何合併 ACI」。

最後，本附錄將列出 `replacement.acis.ldif` 捨棄的 ACI。如需更多資訊，請參閱本附錄後面部分的第 195 頁的 「將要捨棄的未使用之 ACI 清單」。

合併和移除 ACI

本小節中列出的 ldif 檔案 (`replacement.acis.ldif`) 在根字尾處安裝合併的 ACI，並從目錄刪除未使用的 ACI。此 ldif 檔案隨附於位於以下目錄中的 Delegated Administrator：

da_base`/lib/config-templates`

將 `replacement.acis.ldif` 檔案套用至目錄 (使用 `ldapmodify`) 時，`ldapmodify` 指令將移除根字尾處的 `aci` 屬性之所有實例，並用 `replacement.acis.ldif` 檔案中的 ACI 替代這些 ACI。

因此，該程序最初會從根字尾處移除**所有** ACI，並用下面列出的 ACI 集替代它們。如果目錄包含由其他應用程式 (例如，Portal Server) 產生的 ACI，應該將這些 ACI 儲存至檔案，並在套用 `replacement.acis.ldif` 檔案後將其重新套用到該目錄。

如需有關使用此 ldif 檔案清除 ACI 的說明，請參閱第 170 頁的 「替代 ACI 的步驟」。

replacement.acis.ldif 檔案

```
dn: $rootSuffix
changetype: modify
replace: aci
aci: (targetattr = "*")(version 3.0; acl "Configuration Administrator";
```

```
   allow (all)
   userdn="ldap:///uid=admin,ou=Administrators,ou=TopologyManagement,
o=NetscapeRoot";)
aci: (target=""ldap:///$rootSuffix")
  (targetfilter=(!(objectclass=sunServiceComponent)))
  (targetattr != "userPassword||passwordHistory
   ||passwordExpirationTime||passwordExpWarned||passwordRetryCount
  ||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime")
  (version 3.0; acl "anonymous access rights";
   allow (read,search,compare)
   userdn = "ldap:///anyone"; )
aci: (targetattr != "nsroledn||aci||nsLookThroughLimit||nsSizeLimit
  ||nsTimeLimit||nsIdleTimeout||passwordPolicySubentry||passwordExpiration
    Time
  ||passwordExpWarned||passwordRetryCount||retryCountResetTime
  ||accountUnlockTime||passwordHistory||passwordAllowChangeTime||uid||mem
    berOf
  ||objectclass||inetuserstatus||ou||owner||mail||mailuserstatus
  ||memberOfManagedGroup||mailQuota||mailMsgQuota||mailhost
  ||mailAllowedServiceAccess||inetCOS||mailSMTPSubmitChannel")
  (version 3.0; acl "Allow self entry modification";
  allow (write)
  userdn ="ldap:///self";)
aci: (targetattr != " aci || nsLookThroughLimit || nsSizeLimit
  || nsTimeLimit|| nsIdleTimeout")
  (version 3.0; acl "Allow self entry read search";
  allow(write)
  userdn ="ldap:///self";)
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Proxy user rights";
  allow (proxy)
  userdn = "ldap:///cn=puser,ou=DSAME Users,
  $rootSuffix"; )
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS special dsame user rights for all under the root
   suffix";
  allow (all)
  userdn = "ldap:///cn=dsameuser,ou=DSAME Users,
  $rootSuffix"; )
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS special ldap auth user rights";
  allow (read,search)
  userdn = "ldap:///cn=amldapuser,ou=DSAME Users,
  $rootSuffix"; )
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Top-level admin rights";
  allow (all)
  roledn = "ldap:///cn=Top-level Admin Role,
  $rootSuffix"; )
aci: (targetattr="*")
  (version 3.0; acl "Messaging Server End User Administrator Read Only
```

```
   Access";
  allow (read,search)
  groupdn="ldap:///cn=Messaging End User Administrators Group,ou=Groups,
  $rootSuffix";)
aci: (targetattr="objectclass || mailalternateaddress || Mailautoreplymode
   || mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
   || mailforwardingaddress || mailAutoReplyTimeout
   || mailautoreplytextinternal
   || mailautoreplytext || vacationEndDate || vacationStartDate
   || mailautoreplysubject || maxPabEntries || mailMessageStore
   || mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
   || sunUCTimeFormat || mailuserstatus || maildomainstatus")
  (version 3.0; acl "Messaging Server End User Administrator All Access";
  allow (all)
  groupdn = "ldap:///cn=Messaging End User Administrators Group,ou=Groups,
  $rootSuffix";)
aci: (targetattr = "*")
  (version 3.0;acl "Allow Read-Only Access";
  allow (read,search,compare)
  groupdn = "ldap:///cn=Read-Only,ou=Groups,
  $rootSuffix";)
aci: (target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Organization Admin Role access deny";
  deny (write,add,delete,compare,proxy)
  roledn = "ldap:///cn=Organization Admin Role,($dn),
  $rootSuffix";)
aci: (target="ldap:///($dn),$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "Organization Admin Role access allow read";
  allow(read,search)
  roledn = "ldap:///cn=Organization Admin Role,[$dn],
  $rootSuffix" ;)
aci: (target="ldap:///($dn),$rootSuffix")
  (targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
  (entrydn=($dn),$rootSuffix))))
  ( targetattr = "*")
  (version 3.0; acl "S1IS Organization Admin Role access allow";
  allow (all)
  roledn = "ldap:///cn=Organization Admin Role,[$dn],
  $rootSuffix";)
```

替代 ACI 的步驟

開始使用之前

開始使用此程序之前，建議您先檢查目錄中的現有 ACI。應確定是否需要保留將被此程序刪除的任何 ACI。

該程序最初會從根字尾處移除**所有** ACI，並用下面列出的 ACI 集替代它們。如果目錄包含由 Messaging Server 以外的應用程式產生的 ACI，應將這些 ACI 儲存至檔案，並在套用 `replacement.acis.ldif` 檔案後將其重新套用到該目錄。

爲協助您分析由 Access Manager 和 Messaging Server 產生的現有 ACI，請參閱本指南後面部分的以下小節：

- 第 172 頁的 「分析現有 ACI」
- 第 188 頁的 「分析如何合併 ACI」
- 第 195 頁的 「將要捨棄的未使用之 ACI 清單」

替代 ACI

以下程序說明如何在根字尾處合併 ACI 以及移除未使用的 ACI。

▼ 替代 ACI

步驟 **1. 儲存目前在根字尾處的現有 ACI。**

可以使用 `ldapsearch` 指令，如以下範例所示：

```
ldapsearch -D “cn=Directory Manager” -w <password> -s base -b
<$rootSuffix> aci=* aci ><filename>
```

其中，

`<password>` 爲 Directory Server 管理員密碼。

`<$rootSuffix>` 爲根字尾，例如 `o=usergroup`。

`<filename>` 是儲存的 ACI 將要寫入的檔案之名稱。

2. 複製並重新命名 `replacement.acis.ldif` 檔案。

安裝 Delegated Administrator 時，`replacement.acis.ldif` 檔案將安裝在以下目錄中：

da_base `/lib/config-templates`

3. 在 `replacement.acis.ldif` 檔案副本中編輯 `$rootSuffix` 項目。

將根字尾參數 $rootSuffix 變更爲您的根字尾 (例如 `o=usergroup`)。$rootSuffix 參數在 ldif 檔案中多次顯示；必須替代每個實例。

4. 使用 LDAP 目錄工具 `ldapmodify` 替代 ACI。

例如，可以執行以下指令：

```
ldapmodify -D <directory manager> -w <password> -f
<replacement.acis.finished.ldif>
```

其中，

`<directory manager>` 爲 Directory Server 管理員名稱。

<password> 爲 Directory Service 管理員密碼。

<replacement.acis.finished.ldif> 是在目錄中合併和移除 ACI 之已編輯的 ldif 檔案的名稱。

刪除動態組織 ACI

使用 Delegated Administrator 主控台建立組織時，將在組織節點上建立一組 ACI。

在前面程序中安裝的替代 ACI 不需要這些針對組織的 ACI。可以透過使用 Access Manager 主控台阻止建立針對組織的 ACI。

▼ 刪除動態組織 ACI

步驟 1. **做為 `amadmin` 登入 AM 主控台**。
AM 主控台位於以下 URL 中：

`http://<` *machine name*`>:<`*port* `>/amconsole`

其中，

<*machine name*> 是執行 Access Manager 的機器

<*port*> 是連接埠

2. **選取 [服務配置] 標籤**。
依預設，[管理配置] 頁面會顯示。
3. **在主控台右側，向下捲動至 [動態管理角色 ACI]**。
4. **在 [動態管理角色 ACI] 文字方塊中，選取並刪除所有 ACI**。
5. **儲存已編輯的設定**。

分析現有 ACI

本小節中的清單顯示安裝 Access Manager 和 Messaging Server 時安裝在目錄中的 ACI。本小節還說明每個 ACI 的功能，並建議是否保留、合併或捨棄某一 ACI。

ACI 分爲以下種類：

■ 第 173 頁的 「根字尾」

根字尾

```
dn: $rootSuffix
#
# consolidate
#
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry
|| passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime")
(version 3.0; acl "Allow self entry modification except for nsroledn, aci,
resource limit attributes, passwordPolicySubentry and password policy state
attributes";
allow (write)
userdn ="ldap:///self";)
```

動作：合併。

無需此字尾的自我存取權限。此 ACI 是重複的；可以在根字尾處將其併入自我 ACI。

```
#
# retain
#
aci:
(targetattr = "*")
(version 3.0; acl "Configuration Administrator";
allow (all)
userdn = "ldap:///uid=admin, ou=Administrators,
ou=TopologyManagement,o=NetscapeRoot";)
```

動作：保留。

這是「管理」使用者，該使用者將經由通過認證對 slapd-config 實例進行認證。如果使用 comm 和 line 公用程式，所有配置都將做爲 Directory Manager 執行，則不需要此 ACI。如果某人需要做爲此使用者對主控台進行認證，則可以在此處保留該 ACI。可以移除類似的 ACI。

```
-------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------

#
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Configuration Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Configuration Administrators, ou=Groups,
ou=TopologyManagement, o=NetscapeRoot”);)
```

動作：在所有 DB 後端捨棄。

這是「配置管理員」群組，如果主控台用於委派伺服器管理權限，則該群組將具有權限。

```
-------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------

#
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Directory Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Directory Administrators, $rootSuffix”);)
```

動作：在所有 DB 後端捨棄。

這是一般「目錄管理員」群組權限定義。

```
-------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------

#
# discard
#
aci:
(targetattr = “*”)
(version 3.0; acl “SIE Group”;
allow (all)
groupdn = “ldap:///cn=slapd-whater, cn=Sun ONE Directory Server,
cn=Server Group, cn=whater.red.iplanet.com, ou=red.iplanet.com,
o=NetscapeRoot”;)
```

動作：在所有 DB 後端捨棄。

這是主控台/管理伺服器相關群組權限定義。

Access Manager

```
# retain
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Proxy user rights";
allow (proxy)
userdn = "ldap:///cn=puser,ou=DSAME Users,$rootSuffix"; )
```

動作：保留。

此 ACI 可以爲 Access Manager 系統使用者授予存取權限。

```
#
# retain
#
aci:
 (target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the
root suffix";
allow (all)
userdn = "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix"; )
```

動作：保留。

此 ACI 可以爲 Access Manager 系統使用者授予存取權限。

```
#
# retain
#
aci:
(target="ldap:///$rootSuffix")(targetattr="*")|
(version 3.0;acl "S1IS special ldap auth user rights";
allow (read,search)
userdn = "ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix"; )
```

動作：保留。

此 ACI 可以爲 Access Manager 系統使用者授予存取權限。

```
#
# discard
#
aci:
(target="ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix")
(targetattr = "*")
(version 3.0;
acl "S1IS special ldap auth user modify right";
deny (write)
roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 可以阻止頂層管理員 (TLA) 修改 `amldapuser` 帳號。

```
#
# retain
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin rights";
allow (all)
roledn = "ldap:///cn=Top-level Admin Role,$rootSuffix"; )
```

動作：保留。

此 ACI 可以爲頂層管理員角色授予存取權限。

```
#
# discard
#
aci:
(targetattr="iplanet-am-saml-user || iplanet-am-saml-password")
(targetfilter="(objectclass=iplanet-am-saml-service)")
(version 3.0; acl "S1IS Right to modify saml user and password";
deny (all)
(roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix")
AND (userdn != "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix")
AND (userdn != "ldap:///cn=puser,ou=DSAME Users,$rootSuffix"); )
```

動作：捨棄。

此 ACI 可以保護 SAML 相關屬性。

頂層用戶服務管理角色

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

動作：捨棄。

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

動作：捨棄。

頂層策略管理角色

```
#
# discard
#
aci:
target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
```

```
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於頂層策略管理角色。

```
#
# discard
#
aci:
(target="ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access Auth Service
deny";
deny (add,write,delete)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於頂層策略管理角色。

```
#
# discard
#
aci:
(target="ldap:///ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於頂層策略管理角色。

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter="(objectclass=sunismanagedorganization)")
```

```
(targetattr = "sunRegisteredServiceName")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,write,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於頂層策略管理角色。

AM 自身

```
#
# consolidate
#
aci:
(targetattr = "*")
(version 3.0;
acl "S1IS Deny deleting self";
deny (delete)
userdn ="ldap:///self";)
```

動作：合併爲單一自我寫入 ACI。由於一般使用者沒有權限刪除任何項目 (包括其自身)，因此不需要明確拒絕。

這是可以設定自身權限的 ACI 之一。明確拒絕將阻止所有項目刪除自身。

```
#
# consolidate
#
aci:
(targetattr = "objectclass || inetuserstatus
|| iplanet-am-user-login-status
|| iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || iplanet-am-user-account-life
|| iplanet-am-session-max-session-time || iplanet-am-session-max-idle-time
|| iplanet-am-session-get-valid-sessions
|| iplanet-am-session-destroy-sessions
|| iplanet-am-session-add-session-listener-on-all-sessions
|| iplanet-am-user-admin-start-dn
|| iplanet-am-auth-post-login-process-class")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(version 3.0; acl "S1IS User status self modification denied";
deny (write)
userdn ="ldap:///self";)
```

動作：合併爲單一自我寫入 ACI。

這是可以設定自我寫入權限的 ACI 之一。

```
#
# consolidate
#
aci:
(targetattr != "iplanet-am-static-group-dn || uid || nsroledn || aci
|| nsLookThroughLimit || nsSizeLimit || nsTimeLimit || nsIdleTimeout
|| memberOf || iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list")
(version 3.0; acl "S1IS Allow self entry modification except for nsroledn,
aci, and resource limit attributes";
allow (write)
userdn ="ldap:///self";)
```

動作：合併爲單一自我寫入 ACI。

這是可以設定權限的 ACI 之一。

```
#
# consolidate
#
aci:
(targetattr != "aci || nsLookThroughLimit || nsSizeLimit || nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow")
(version 3.0; acl "S1IS Allow self entry read search except for nsroledn,
aci, resource limit and web agent policy attributes";
allow (read,search)
userdn ="ldap:///self";)
```

動作：合併爲單一自我寫入 ACI。

這是可以設定自我寫入權限的 ACI 之一。

AM 匿名

```
#
# consolidate
#
```

```
aci:
(target="ldap:///ou=services,$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr = "*")
(version 3.0; acl "S1IS Services anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

動作：合併爲單一匿名 ACI。

這是可以授予匿名權限的 ACI 之一。

```
#
# consolidate
#
aci:
(target="ldap:///ou=iPlanetAMAdminConsoleService,*,$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS iPlanetAMAdminConsoleService anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

動作：合併爲單一匿名 ACI。

這是可以授予匿名權限的 ACI 之一。

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )
```

動作：捨棄。

此 ACI 可以阻止任何使用者 (`rootdn` 之外) 刪除預設組織。

```
#
# discard
#
```

```
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin delete right denied";
deny(delete)
userdn = "ldap:///anyone"; )
```

動作：捨棄。

此 ACI 可阻止任何使用者 (rootdn 之外) 刪除頂層管理員角色。

AM 拒絕寫入存取權限

```
#
# discard
#
aci: (targetattr = "*")
(version 3.0; acl "S1IS Deny write to anonymous user";
deny (add,write,delete)
roledn ="ldap:///cn=Deny Write Access,$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於拒絕寫入存取權限角色。

AM 容器管理角色

```
#
# discard
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Container Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Container Admin Role,[$dn],$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於容器管理角色。

```
-----------------------------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------------------------

#
# discard
#
aci:
(target="ldap:///cn=Container Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Container Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Container Admin Role,($dn),$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於容器管理角色。

```
-----------------------------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------------------------

#
# discard
#
aci:
 (target="ldap:///ou=People,$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix)
(nsroledn=cn=Container Admin Role,$rootSuffix))))
(targetattr != "iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn")
(version 3.0; acl "S1IS Group and people container admin role";
allow (all)
roledn = "ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com,$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於群組和使用者容器管理角色。

```
-----------------------------------------------------------------------------------------------------------
```

組織用戶服務

```
-----------------------------------------------------------------------------------------------------------

#
# discard
#
aci: (extra verses dreambig)
(target="ldap:///$rootSuffix")
```

```
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於組織用戶服務管理角色。

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)
```

動作：捨棄。

此 ACI 適用於組織用戶服務管理角色。

AM 組織管理角色

```
#
# consolidate
#
aci: (different name - "allow all" instead of "allow")
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn ="ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

動作：合併。

```
#
# consolidate
#
aci:
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)
```

動作：合併。

此 ACI 適用於組織管理角色。

```
#
# consolidate
#
aci: (missing)
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to org node";
allow (read,search)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

動作：合併。

此 ACI 適用於組織管理角色。

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

動作：合併。

此 ACI 適用於組織管理角色。

```
-------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------

#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr!="businessCategory || description || facsimileTelephoneNumber
|| postalAddress || preferredLanguage || searchGuide || postOfficeBox ||
postalCode
|| registeredaddress || street || l || st || telephonenumber
||maildomainreportaddress
|| maildomainwelcomemessage || preferredlanguage || sunenablegab")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

動作：合併。

此 ACI 適用於組織管理角色。

```
-------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------

#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

動作：合併。

```
-------------------------------------------------------------------------------------------------------
```

AM 其他

```
-------------------------------------------------------------------------------------------------------

#
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetattr!="nsroledn")
```

```
(version 3.0; acl "S1IS Group admin's right to the users he creates";
allow (all)
userattr = "iplanet-am-modifiable-by#ROLEDN";)
```

動作：捨棄。

捨棄此 ACI 將停用與 `iplanet-am-modifiable-by` 屬性關聯的權限。

Messaging Server

```
#
# consolidate
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator Read
Access Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1";
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix";)
```

動作：合併。

此 ACI 可以授予郵件傳送一般使用者管理員群組權限。

```
#
# consolidate
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="objectclass||mailalternateaddress||mailautoreplymode
||mailprogramdeliveryinfo||nswmextendeduserprefs||preferredlanguage
||maildeliveryoption||mailforwardingaddress
||mailAutoReplyTimeout||mailautoreplytextinternal||mailautoreplytext
||vacationEndDate||vacationStartDate||mailautoreplysubject||pabURI
||maxPabEntries||mailMessageStore||mailSieveRuleSource||sunUCDateFormat
||sunUCDateDeLimiter||sunUCTimeFormat")
(version 3.0; acl "Messaging Server End User Adminstrator Write
Access Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1";
allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix";)
```

動作：合併。

此 ACI 可以授予郵件傳送一般使用者管理員群組權限。

```
#
# consolidate
#
aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress
||mailEquivalentAddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota||inetSubscriberAccountId||dataSource||mailhost
||mailAllowedServiceAcces||pabURI||inetCOS||mailSMTPSubmitChannel
||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization
Admin Role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)
```

動作：合併。

這是可以設定自身權限的 ACI 之一。

分析如何合併 ACI

本小節中的清單顯示在替代 ldif 檔案 `replacement.acis.ldif` (可以使用該檔案在目錄中合併 ACI) 中已合併的 ACI。如需有關如何替代 ACI 的說明，請參閱第 170 頁的「替代 ACI 的步驟」。

ACI 分爲幾對。對於每一種類，將先列出原始 ACI，然後列出合併後的 ACI：

原始匿名存取權限

```
aci:
(targetattr != "userPassword || passwordHistory || passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordAllowChangeTime ")
(version 3.0; acl "Anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)

aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
version 3.0; acl "S1IS Top-level admin delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )


aci:
(target="ldap:///$rootSuffix")
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )


aci:
(target="ldap:///ou=services,$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr = "*")
(version 3.0; acl "S1IS Services anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)


aci:
(target="ldap:///ou=iPlanetAMAdminConsoleService,*,$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS iPlanetAMAdminConsoleService anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

合併後的匿名存取權限

```
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr != "userPassword||passwordHistory
||passwordExpirationTime||passwordExpWarned||passwordRetryCount
||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime")
(version 3.0; acl "anonymous access rights";
allow (read,search,compare)
userdn = "ldap:///anyone"; )
```

分析：此 ACI (位於根中) 允許與原始匿名 ACI 集合相同的存取權限。此 ACI 透過列出一組排除的屬性清單來執行此作業。此替代 ACI 可以透過在目標中刪除 (*) 來提昇效能。

原始自我 ACI

```
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordHistory || passwordAllowChangeTime")
(version 3.0; acl "Allow self entry modification except for nsroledn, aci,
resource limit attributes, passwordPolicySubentry and password policy
state attributes";
allow (write)
userdn ="ldap:///self";)


aci:
(targetattr = "*")
(version 3.0; acl "S1IS Deny deleting self";
deny (delete)
userdn ="ldap:///self";)


aci:
(targetattr = "objectclass || inetuserstatus ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list
|| iplanet-am-user-account-life || iplanet-am-session-max-session-time
|| iplanet-am-session-max-idle-time
|| iplanet-am-session-get-valid-sessions
|| iplanet-am-session-destroy-sessions
|| iplanet-am-session-add-session-listener-on-all-sessions
|| iplanet-am-user-admin-start-dn
|| iplanet-am-auth-post-login-process-class")
(targetfilter=(!(nsroledn=cn=Top-levelAdmin Role,$rootSuffix)))
(version 3.0; acl "S1IS User status self modification denied";
deny (write)
userdn ="ldap:///self";)


aci:
(targetattr != "iplanet-am-static-group-dn || uid || nsroledn || aci
|| LookThroughLimit
|| nsSizeLimit || nsTimeLimit || nsIdleTimeout || memberOf ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow ||
planet-am-web-agent-access-deny-list")
(version 3.0; acl "S1IS Allow self entry modification except
for nsroledn, aci, and resource limit attributes";
```

```
allow (write)
userdn =”ldap:///self”;)


aci:
(targetattr != “aci || nsLookThroughLimit || nsSizeLimit || nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow”)
(version 3.0; acl “S1IS Allow self entry read search except for
nsroledn, aci, resource limit and web agent policy attributes”;
allow (read,search)
userdn =”ldap:///self”;)


aci:
(targetattr=”uid||ou||owner||mail||mailAlternateAddress
||mailEquivalentaddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
||pabURI||inetCOS||mailSMTPSubmitChannel||aci”)
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization Admin
role,*))))
(version 3.0; acl “Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 “;
deny (write)
userdn = “ldap:///self”;)
```

合併後的自我 ACI

```
aci:
(targetattr != “nsroledn || aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
asswordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime ||
id || memberOf
|| objectclass || inetuserstatus || ou || owner || mail || mailuserstatus
|| memberOfManagedGroup ||mailQuota || mailMsgQuota || mailhost
|| mailAllowedServiceAccess || inetCOS || mailSMTPSubmitChannel”)
(version 3.0; acl “Allow self entry modification”;
allow (write)
userdn =”ldap:///self”;)


aci:
(targetattr != “ aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit|| nsIdleTimeout”)
(version 3.0; acl “Allow self entry read search”;
allow(read,search)
userdn =”ldap:///self”;)
```

分析：缺少所有 `iplanet-am-*` 屬性。由於 `deny` 是預設值 (如果 ACI 不存在)，因此將移除所有 `deny` ACI。允許 `write` 的所有 ACI 將被合併爲單一 ACI。

原始 Messaging Server ACI

```
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator Read
Access Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1";
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
rootSuffix";)


aci:
(target="ldap:///$rootSuffix")
(targetattr="objectclass||mailalternateaddress||mailautoreplymode||
mailprogramdeliveryinfo
||nswmextendeduserprefs||preferredlanguage||maildeliveryoption||
mailforwardingaddress
||mailAutoReplyTimeout||mailautoreplytextinternal||mailautoreplytext||
vacationEndDate
||vacationStartDate||mailautoreplysubject||pabURI||maxPabEntries||
mailMessageStore
||mailSieveRuleSource||sunUCDateFormat||sunUCDateDeLimiter||
sunUCTimeFormat")
(version 3.0; acl "Messaging Server End User Adminstrator Write
Access Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1";
allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
rootSuffix";)


aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress||
mailEquivalentAddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota||
mailMsgQuota
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
||pabURI||inetCOS||mailSMTPSubmitChannel||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization Admin
Role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)
```

合併後的 Messaging Server ACI

將在自我 ACI 中處理自我 ACI。

```
aci:
(targetattr="*")
```

```
(version 3.0; acl "Messaging Server End User Administrator
Read Only Access";
allow (read,search)
groupdn = "ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix"; )


aci:
(targetattr="objectclass || mailalternateaddress || Mailautoreplymode
|| mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
|| mailforwardingaddress || mailAutoReplyTimeout
|| mailautoreplytextinternal
|| mailautoreplytext || vacationEndDate || vacationStartDate
|| mailautoreplysubject || maxPabEntries || mailMessageStore
|| mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
|| sunUCTimeFormat || mailuserstatus || maildomainstatus")
(version 3.0; acl "Messaging Server End User Administrator All Access";
allow (all)
groupdn = "ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix";)
```

分析：與原始 ACI 相同。

原始組織管理 ACI

```
aci: (different name - "allow all" instead of "allow")
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn ="ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)


aci: (missing)
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to org node";
allow (read,search)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

```
aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr!="businessCategory || description || facsimileTelephoneNumber
|| postalAddress || preferredLanguage || searchGuide || postOfficeBox
|| postalCode
|| registeredaddress || street || l || st || telephonenumber
|| maildomainreportaddress
|| maildomainwelcomemessage || preferredlanguage || sunenablegab")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)


aci: (duplicate of per organization aci)
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)


aci:
(target="ldap:///cn=Organization Admin
Role,($dn),dc=red,dc=iplanet,dc=com")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)


aci:
(target="ldap:///o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,
o=Business,rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=red,dc=iplanet,dc=com))))
(targetattr = "nsroledn")
(targattrfilters="add=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe.com,
o=SharedDomainsRoot,o=Business,$rootSuffix),
del=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,
o=Business,$rootSuffix)")
(version 3.0;
acl "S1IS Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin
Role,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,o=Business,
$rootSuffix";)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
```

```
allow (all)
roledn = "ldap:///cn=Organization Admin
Role,[$dn],dc=red,dc=iplanet,dc=com";)
```

合併後的組織管理 ACI

```
aci:
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read";
allow(read,search)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix" ;)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(entrydn=($dn),$rootSuffix))))
( targetattr = "*")
(version 3.0; acl "S1IS Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

將要捨棄的未使用之 ACI 清單

本小節中的清單顯示在將 `replacement.acis.ldif` 檔案套用至目錄時要捨棄的未使用之預設 ACI。

要捨棄的 ACI 分爲以下種類：

字尾

```
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Configuration Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Configuration Administrators, ou=Groups,
ou=TopologyManagement, o=NetscapeRoot”);)


#
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Directory Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Directory Administrators, $rootSuffix”);)


#
# discard
#
aci:
(targetattr = “*”)
(version 3.0;
acl “SIE Group”;
allow (all)
groupdn = “ldap:///cn=slapd-whater, cn=Sun ONE Directory Server, cn=Server
Group, cn=whater.red.iplanet.com, ou=red.iplanet.com, o=NetscapeRoot”;)


#
# discard - prevents TLA from modifying the amldapuser account.
#
aci:
(target=”ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix”)
(targetattr = “*”)
(version 3.0;
acl “S1IS special ldap auth user modify right”;
deny (write)
roledn != “ldap:///cn=Top-level Admin Role,$rootSuffix”;)


#
# discard - protects SAML related attributes
#
aci:
(targetattr=”iplanet-am-saml-user || iplanet-am-saml-password”)
(targetfilter=”(objectclass=iplanet-am-saml-service)”)
(version 3.0; acl “S1IS Right to modify saml user and password”;
deny (all)
(roledn != “ldap:///cn=Top-level Admin Role,$rootSuffix”)
```

```
AND (userdn != "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix")
AND (userdn != "ldap:///cn=puser,ou=DSAME Users,$rootSuffix"); )
```

頂層用戶服務管理角色

```
#
# discard
 #
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

頂層策略管理角色

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access
Auth Service deny";
deny (add,write,delete)
```

```
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter="(objectclass=sunismanagedorganization)")
(targetattr = "sunRegisteredServiceName")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,write,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

Access Manager 匿名

```
#
# discard - prevents anyone other than rootdn from deleting
# default organization.
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )


#
# discard - prevents any user other than rootdn from deleting the
# TLA admin role.
#
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
version 3.0; acl "S1IS Top-level admin delete right denied";
deny(delete)
userdn = "ldap:///anyone"; )
```

Access Manager 拒絕寫入存取權限

```
#
# discard
```

```
#
aci:
(targetattr = "*")
(version 3.0; acl "S1IS Deny write to anonymous user";
deny (add,write,delete)
roledn ="ldap:///cn=Deny Write Access,$rootSuffix";)
```

Access Manager 容器管理角色

```
#
# discard
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Container Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Container Admin Role,[$dn],$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///cn=Container Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Container Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Container Admin Role,($dn),$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///ou=People,$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix)
(nsroledn=cn=Container Admin Role,$rootSuffix))))
(targetattr != "iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn")
(version 3.0; acl "S1IS Group and people container admin role";
allow (all)
roledn = "ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com,$rootSuffix";)
```

組織用戶服務

```
#
# discard
```

```
#
aci: (extra verses dreambig)
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)
```

Access Manager 其他

```
#
# discard - Removal disables the associated privileges to the attribute
# iplanetam-modifiable-by
#
aci:
(target="ldap:///$rootSuffix")
(targetattr!="nsroledn")
(version 3.0; acl "S1IS Group admin's right to the users he creates";
allow (all)
userattr = "iplanet-am-modifiable-by#ROLEDN";)
```

索引

I

J

L

M

N

R

S

U

W